# Assessment Results

## FISMA

NOTE: The format of the FISMA portion of this **TECH LOCK**® Certified Report is designed to be identical to the format of the Security Assessment Report (“SAR”) that the U.S. Department of Education requires its subcontractors to use.

The RESULTS column contains either an “S” (for a Satisfactory rating), or an “OS” (for an Other than Satisfactory rating). A rating of “S” indicates that the control is In Place. A rating of “OS” indicates that there are one or more findings or non-conformities for the control.

### Access Control (AC)

|  |  |  |
| --- | --- | --- |
| **AC-1** | **ACCESS CONTROL POLICY AND PROCEDURES** | **RESULTS** |
| **AC-1.1** | Determine if: |  |
| **AC-1.1.1** | 1. the organization develops and formally documents access control policy; |  |
| **AC-1.1.2** | 1. the organization access control policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **AC-1.1.3** | 1. the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities; |  |
| **AC-1.1.4** | 1. the organization develops and formally documents access control procedures; |  |
| **AC-1.1.5** | 1. the organization access control procedures facilitate implementation of the access control policy and associated access control controls; and |  |
| **AC-1.1.6** | 1. the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities. |  |
| **AC-1.2** | Determine if: |  |
| **AC-1.2.1** | 1. the organization defines the frequency of access control policy reviews/updates; |  |
| **AC-1.2.2** | 1. the organization reviews/updates access control policy in accordance with organization-defined frequency; and |  |
| **AC-1.2.3** | 1. the organization defines the frequency of access control procedure reviews/updates; |  |
| **AC-1.2.4** | 1. the organization reviews/updates access control procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2** | **ACCOUNT MANAGEMENT** | **RESULTS** |
| **AC-2.1** | Determine if: |  |
| **AC-2.1.1** | 1. the organization manages information system accounts, including;  * identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); * establishing conditions for group membership; * identifying authorized users of the information system and specifying access privileges; * requiring appropriate approvals for requests to establish accounts; * establishing, activating, modifying, disabling, and removing accounts; * specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; * notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; * deactivating: i) temporary accounts that are no longer required; and ii) accounts of terminated or transferred users; and * granting access to the system based on: * a valid access authorization; * intended system usage; and * other attributes as required by the organization or associated missions/business functions; and |  |
| **AC-2.1.2** | 1. the organization defines the frequency of information system account reviews; and |  |
| **AC-2.1.3** | 1. the organization reviews information system accounts in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(1)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(1).1** | Determine if the organization employs automated mechanisms to support information system account management functions. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(2)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(2).1** | Determine if: |  |
| **AC-2(2).1.1** | 1. the organization defines in the security plan, explicitly or by reference, a time period for each type of account after which the information system terminates temporary and emergency accounts; and |  |
| **AC-2(2).2.1** | 1. the information system automatically terminates temporary and emergency accounts after the organization-defined time period for each type of account. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(3)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(3).1** | Determine if: |  |
| **AC-2(3).1.1** | 1. the organization defines in the security plan, explicitly or by reference, a time period after which the information system disables inactive accounts; and |  |
| **AC-2(3).2.1** | 1. the information system automatically disables inactive accounts after organization-defined time period. |  |

|  |  |  |
| --- | --- | --- |
| **AC-2(4)** | **ACCOUNT MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-2(4).1** | Determine if: |  |
| **AC-2(4).1.1** | 1. the information system automatically audits:  * account creation; * modification; * disabling; and * termination actions; and |  |
| **AC-2(4).1.2** | 1. the information system notifies, as required, appropriate individuals. |  |

|  |  |  |
| --- | --- | --- |
| **AC-3** | **ACCESS ENFORCEMENT** | **RESULTS** |
| **AC-3.1** | Determine if the information system enforces approved authorizations for logical access  to the system in accordance with applicable policy. |  |

|  |  |  |
| --- | --- | --- |
| **AC-4** | **INFORMATION FLOW ENFORCEMENT** | **RESULTS** |
| **AC-4.1** | Determine if: |  |
| **AC-4.1.1** | 1. The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; |  |

|  |  |  |
| --- | --- | --- |
| **AC-5** | **SEPARATION OF DUTIES** | **RESULTS** |
| **AC-5.1** | Determine if: |  |
| **AC-5.1.1** | 1. the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and |  |
| **AC-5.1.2** | 1. the information system enforces separation of duties through assigned access authorizations. |  |

|  |  |  |
| --- | --- | --- |
| **AC-6** | **LEAST PRIVILEGE** | **RESULTS** |
| **AC-6.1** | Determine if: |  |
| **AC-6.1.1** | 1. the organization assigns the most restrictive set of rights/privileges or accesses needed by the users for the performance of specified tasks; and |  |
| **AC-6.1.2** | 1. the information system enforces the most restrictive set of rights/privileges or accesses needed by users. |  |

|  |  |  |
| --- | --- | --- |
| **AC-6(1)** | **LEAST PRIVILEGE – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-6(1).1** | Determine if: |  |
| **AC-6(1).1.1** | 1. the organization defines the security functions (deployed in hardware, software, and   firmware) and security-relevant information for which access must be explicitly  authorized; and |  |
| **AC-6(1).1.2** | 1. the organization explicitly authorizes access to the organization-defined security   functions and security-relevant information. |  |

|  |  |  |
| --- | --- | --- |
| **AC-6(2)** | **LEAST PRIVILEGE – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-6(2).1** | Determine if: |  |
| **AC-6(2).1.1** | 1. the organization defines the security functions or security-relevant information to   which users of information system accounts, or roles, have access; and |  |
| **AC-6(2).1.2** | 1. the organization requires that users of information system accounts, or roles, with   access to organization-defined security functions or security-relevant information,  use non-privileged accounts, or roles, when accessing other system functions; and |  |
| **AC-6(2).1.3** | 1. the organization, if deemed feasible, audits any use of privileged accounts, or roles,   with access to organization-defined security functions or security-relevant  information, when accessing other system functions. |  |

|  |  |  |
| --- | --- | --- |
| **AC-7** | **UNSUCCESSFUL LOGIN ATTEMPTS** | **RESULTS** |
| **AC-7.1** | Determine if: |  |
| **AC-7.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur; |  |
| **AC-7.1.2** | 1. the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period; |  |
| **AC-7.1.3** | 1. the organization defines in the security plan, explicitly or by reference, the time period for lock out mode or delay period; |  |
| **AC-7.1.4** | 1. the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; and |  |
| **AC-7.1.5** | 1. the information system enforces the organization-selected lock out mode or delayed login prompt. |  |

|  |  |  |
| --- | --- | --- |
| **AC-8** | **SYSTEM USE NOTIFICATION** | **RESULTS** |
| **AC-8.1** | Determine if: |  |
| **AC-8.1.1** | 1. the information system displays a system use notification message before granting system access informing potential users:  * that the user is accessing a U.S. Government information system; * that the system usage may be monitored, recorded and subject to audit; * that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and * that the use of the system indicates consent to monitoring and recording; |  |
| **AC-8.1.2** | 1. the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries); |  |
| **AC-8.1.3** | 1. the organization approves the information system use notification message before its use; and |  |
| **AC-8.1.4** | 1. the system use notification message remains on the screen until the users take explicit action to log on to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-11** | **SESSION LOCK** | **RESULTS** |
| **AC-11.1** | Determine if: |  |
| **AC-11.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the time period of user inactivity after which the information system initiates a session lock; |  |
| **AC-11.1.2** | 1. the information system initiates a session lock after the organization-defined time period of inactivity; |  |
| **AC-11.1.3** | 1. the information system provides the capability for users to directly initiate session lock mechanisms; and |  |
| **AC-11.1.4** | 1. the information system maintains the session lock until the user reestablishes access using the appropriate identification and authentication procedures. |  |

|  |  |  |
| --- | --- | --- |
| **AC-14** | **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION** | **RESULTS** |
| **AC-14.1** | Determine if: |  |
| **AC-14.1.1** | 1. the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication. |  |

|  |  |  |
| --- | --- | --- |
| **AC-14(1)** | **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION** | **RESULTS** |
| **AC-14(1).1** | Determine if: |  |
| **AC-14(1).1.1** | 1. the organization permits action to be performed without identification and authentication only to the extent necessary to accomplish mission objectives. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17** | **REMOTE ACCESS** | **RESULTS** |
| **AC-17.1** | Determine if: |  |
| **AC-17.1.1** | 1. the organization authorizes, monitors, and controls remote access to the information system for all allowed methods of remote access to include both establishment of the remote connection and subsequent user actions across that connection. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(1)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(1).1** | Determine if: |  |
| **AC-17(1).1.1** | 1. The information system employs automated mechanisms to facilitate the monitoring and control of remote access methods. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(2)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(2).1** | Determine if: |  |
| **AC-17(2).1.1** | 1. the information system employs cryptography to protect the confidentiality and integrity of remote access sessions. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(3)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(3).1** | Determine if: |  |
| **AC-17(3).1.1** | 1. the organization defines managed access control points for remote access to the information system; and |  |
| **AC-17(3).2.1** | 1. the information system controls all remote access through a limited number of managed access control points. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(4)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(4).1** | Determine if: |  |
| **AC-17(4).1.1** | 1. the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and |  |
| **AC-17(4).2.1** | 1. the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(5)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(5).1** | Determine if: |  |
| **AC-17(5).1.1** | 1. The organization monitors for unauthorized remote connections to the information system [Assignment: organization-defined frequency], and takes appropriate action if an unauthorized connection is discovered. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(7)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(7).1** | Determine if: |  |
| **AC-17(7).1.1** | 1. The organization ensures that remote sessions for accessing [Assignment: organization-defined list of security functions and security-relevant information] employ [Assignment: organization defined additional security measures] and are audited. |  |

|  |  |  |
| --- | --- | --- |
| **AC-17(8)** | **REMOTE ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-17(8).1** | Determine if: |  |
| **AC-17(8).1.1** | 1. The organization disables all unnecessary ports and protocols except for explicitly identified components in support of specific operational requirements. |  |

|  |  |  |
| --- | --- | --- |
| **AC-18** | **WIRELESS ACCESS** | **RESULTS** |
| **AC-18.1** | Determine if: |  |
| **AC-18.1.1** | 1. the organization establishes usage restrictions and implementation guidance for wireless technologies; |  |
| **AC-18.1.2** | 1. the organization authorizes, monitors, and controls wireless access to the information system; and |  |
| **AC-18.1.3** | 1. the wireless access restrictions are consistent with NIST Special Publications 800-48 and 800-97 |  |

|  |  |  |
| --- | --- | --- |
| **AC-18(1)** | **WIRELESS ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-18(1).1** | Determine if: |  |
| **AC-18(1).1.1** | 1. the organization uses authentication and encryption to protect wireless access to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19** | **ACCESS CONTROL FOR MOBILE DEVICES** | **RESULTS** |
| **AC-19.1** | Determine if: |  |
| **AC-19.1.1** | 1. the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and |  |
| **AC-19.1.2** | 1. the organization authorizes, monitors, and controls device access to organizational information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19(1)** | **ACCESS CONTROL FOR MOBILE DEVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-19(1).1** | Determine if: |  |
| **AC-19(1).1.1** | 1. The organization restricts the use of writable, removable media in organizational information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19(2)** | **ACCESS CONTROL FOR MOBILE DEVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-19(2).1** | Determine if: |  |
| **AC-19(2).1.1** | 1. The organization prohibits the use of personally owned, removable media in organizational information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-19(3)** | **ACCESS CONTROL FOR MOBILE DEVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-19(3).1** | Determine if: |  |
| **AC-19(3).1.1** | 1. The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner. |  |

|  |  |  |
| --- | --- | --- |
| **AC-20** | **USE OF EXTERNAL INFORMATION SYSTEMS** | **RESULTS** |
| **AC-20.1** | Determine if: |  |
| **AC-20.1.1** | 1. the organization establishes terms and conditions for authorized individuals to access the information system from an external system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-20(1)** | **USE OF EXTERNAL INFORMATION SYSTEMS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-20(1).1** | Determine if: |  |
| **AC-20(1).1.1** | 1. the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:  * verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization’s information security policy and system security plan when allowing connections to the external information system; or * approves, for authorized exceptions, information system connection or processing agreements with the organizational entity hosting the external information system. |  |

|  |  |  |
| --- | --- | --- |
| **AC-20(2)** | **USE OF EXTERNAL INFORMATION SYSTEMS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AC-20(2).1** | Determine if the organization limits the use of organization-controlled portable storage  media by authorized individuals on external information systems. |  |

|  |  |  |
| --- | --- | --- |
| **AC-22** | **PUBLICLY ACCESSIBLE CONTENT** | **RESULTS** |
| **AC-22.1** | Determine if: |  |
| **AC-22.1.1** | 1. the organization designates individuals authorized to post information onto an organizational information system that is publicly accessible; |  |
| **AC-22.1.2** | 1. the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; |  |
| **AC-22.1.3** | 1. the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; |  |
| **AC-22.1.4** | 1. the organization defines the frequency of reviews of the content on the publicly accessible organizational information system for nonpublic information; |  |
| **AC-22.1.5** | 1. the organization reviews the content on the publicly accessible organizational information system for nonpublic information in accordance with the organization defined frequency; and |  |
| **AC-22.1.6** | 1. the organization removes nonpublic information from the publicly accessible organizational information system, if discovered. |  |

### Security Awareness and Training (AT)

|  |  |  |
| --- | --- | --- |
| **AT-1** | **SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES** | **RESULTS** |
| **AT-1.1** | Determine if: |  |
| **AT-1.1.1** | 1. the organization develops and formally documents awareness and training policy; |  |
| **AT-1.1.2** | 1. the organization awareness and training policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **AT-1.1.3** | 1. the organization disseminates formal documented awareness and training policy to elements within the organization having associated awareness and training roles and responsibilities; |  |
| **AT-1.1.4** | 1. the organization develops and formally documents awareness and training procedures; |  |
| **AT-1.1.5** | 1. the organization awareness and training procedures facilitate implementation of the awareness and training policy and associated awareness and training controls; and |  |
| **AT-1.1.6** | 1. the organization disseminates formal documented awareness and training procedures to elements within the organization having associated awareness and training roles and responsibilities. |  |
| **AT-1.2** | Determine if: |  |
| **AT-1.2.1** | 1. the organization defines the frequency of awareness and training policy reviews/updates; |  |
| **AT-1.2.2** | 1. the organization reviews/updates awareness and training policy in accordance with organization-defined frequency; and |  |
| **AT-1.2.3** | 1. the organization defines the frequency of awareness and training procedure reviews/updates; |  |
| **AT-1.2.4** | 1. the organization reviews/updates awareness and training procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AT-2** | **SECURITY AWARENESS** | **RESULTS** |
| **AT-2.1** | Determine if: |  |
| **AT-2.1.1** | 1. the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes; |  |
| **AT-2.1.2** | 1. the security awareness training is consistent with applicable regulations and NIST Special Publication 800-50; |  |
| **AT-2.1.3** | 1. the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access; |  |
| **AT-2.1.4** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually; and |  |
| **AT-2.1.5** | 1. the organization provides refresher security awareness training in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AT-3** | **SECURITY TRAINING** | **RESULTS** |
| **AT-3.1** | Determine if: |  |
| **AT-3.1.1** | 1. the organization identifies personnel with significant information system security responsibilities and roles and documents those roles and responsibilities; |  |
| **AT-3.1.2** | 1. the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties when required by system changes; |  |
| **AT-3.1.3** | 1. the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security; |  |
| **AT-3.1.4** | 1. the security training is consistent with applicable regulations and NIST Special Publication 800-50; |  |
| **AT-3.1.5** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of refresher security training; and |  |
| **AT-3.1.6** | 1. the organization provides refresher security training in accordance with organization-defined frequency, at least annually. |  |

|  |  |  |
| --- | --- | --- |
| **AT-4** | **SECURITY TRAINING RECORDS** | **RESULTS** |
| **AC-4.1** | Determine if: |  |
| **AT-4.1.1** | 1. the organization monitors and documents basic security awareness training and specific information system security training. |  |

### Audit and Accountability (AU)

|  |  |  |
| --- | --- | --- |
| **AU-1** | **AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES** | **RESULTS** |
| **AU-1.1** | Determine if: |  |
| **AU-1.1.1** | 1. the organization develops and formally documents audit and accountability policy; |  |
| **AU-1.1.2** | 1. the organization audit and accountability policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **AU-1.1.3** | 1. the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities; |  |
| **AU-1.1.4** | 1. the organization develops and formally documents audit and accountability procedures; |  |
| **AU-1.1.5** | 1. the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls; and |  |
| **AU-1.1.6** | 1. the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities. |  |
| **AU-1.2** | Determine if: |  |
| **AU-1.2.1** | 1. the organization defines the frequency of audit and accountability policy reviews/updates; |  |
| **AU-1.2.2** | 1. the organization reviews/updates audit and accountability policy in accordance with organization-defined frequency; and |  |
| **AU-1.2.3** | 1. the organization defines the frequency of audit and accountability procedure reviews/updates; |  |
| **AU-1.2.4** | 1. the organization reviews/updates audit and accountability procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AU-2** | **AUDITABLE EVENTS** | **RESULTS** |
| **AU-2.1** | Determine if: |  |
| **AU-2.1.1** | 1. the organization defines in the security plan, explicitly or by reference, information system auditable events; |  |
| **AU-2.1.2** | 1. the organization-defined auditable events include those deemed by the organization to be adequate to support after-the-fact investigations of security incidents; |  |
| **AU-2.1.3** | 1. the information system generates audit records for the organization-defined auditable events; |  |
| **AU-2.1.4** | 1. the organization specifies which information system components carry out auditing activities; and |  |
| **AU-2.1.5** | 1. the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. |  |

|  |  |  |
| --- | --- | --- |
| **AU-2(3)** | **AUDITABLE EVENTS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-2(3).1** | Determine if: |  |
| **AU-2(3).1.1** | 1. the organization periodically reviews and updates the list of organization-defined auditable events. |  |

|  |  |  |
| --- | --- | --- |
| **AU-2(4)** | **AUDITABLE EVENTS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-2(4).1** | Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system. |  |

|  |  |  |
| --- | --- | --- |
| **AU-3** | **CONTENT OF AUDIT RECORDS** | **RESULTS** |
| **AU-3.1** | Determine if: |  |
| **AU-3.1.1** | 1. the information system audit records capture sufficient information to establish what events occurred; |  |
| **AU-3.1.2** | 1. the information system audit records capture sufficient information to establish the sources of the events; and |  |
| **AU-3.1.3** | 1. the information system audit records capture sufficient information to establish the outcomes of the events. |  |

|  |  |  |
| --- | --- | --- |
| **AU-3(1)** | **CONTENT OF AUDIT RECORDS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-3(1).1** | Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. |  |

|  |  |  |
| --- | --- | --- |
| **AU-4** | **AUDIT STORAGE CAPACITY** | **RESULTS** |
| **AU-4.1** | Determine if: |  |
| **AU-4.1.1** | 1. the organization allocates sufficient audit record storage capacity; and |  |
| **AU-4.2.1** | 1. the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded. |  |

|  |  |  |
| --- | --- | --- |
| **AU-5** | **RESPONSE TO AUDIT PROCESSING FAILURES** | **RESULTS** |
| **AU-5.1** | Determine if: |  |
| **AU-5.1.1** | 1. the organization defines in the security plan, explicitly or by reference, actions to be taken in the event of an audit processing failure; |  |
| **AU-5.1.2** | 1. the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure; and |  |
| **AU-5.1.3** | 1. the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure, to include audit storage capacity being reached or exceeded. |  |

|  |  |  |
| --- | --- | --- |
| **AU-6** | **AUDIT REVIEW, ANALYSIS, AND REPORTING** | **RESULTS** |
| **AU-6.1** | Determine if: |  |
| **AU-6.1.1** | 1. the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity; |  |
| **AU-6.1.2** | 1. the organization investigates suspicious activity or suspected violations; |  |
| **AU-6.1.3** | 1. the organization report’s findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and |  |
| **AU-6.1.4** | 1. the organization takes necessary actions in response to the reviews/analyses of audit records. |  |
| **AU-6.2.1** | 1. the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources. |  |

|  |  |  |
| --- | --- | --- |
| **AU-7** | **AUDIT REDUCTION AND REPORT GENERATION** | **RESULTS** |
| **AU-7.1** | Determine if the information system provides audit reduction and report generation tools that support after-the-fact investigations of security incidents without altering original audit records. |  |

|  |  |  |
| --- | --- | --- |
| **AU-7(1)** | **AUDIT REDUCTION AND REPORT GENERATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-7(1).1** | Determine if the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria. |  |

|  |  |  |
| --- | --- | --- |
| **AU-8** | **TIME STAMPS** | **RESULTS** |
| **AU-8.1** | Determine if the information system provides time stamps in audit records. |  |

|  |  |  |
| --- | --- | --- |
| **AU-8(1)** | **TIME STAMPS – CONTROL ENHANCEMENT** | **RESULTS** |
| **AU-8(1).1** | Determine if: |  |
| **AU-8(1).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of internal clock synchronization for the information system; and |  |
| **AU-8(1).2.1** | 1. the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **AU-9** | **PROTECTION OF AUDIT INFORMATION** | **RESULTS** |
| **AU-9.1** | Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion. |  |

|  |  |  |
| --- | --- | --- |
| **AU-11** | **AUDIT RECORD RETENTION** | **RESULTS** |
| **AU-11.1** | Determine if: |  |
| **AU-11.1.1** | 1. the organization defines the retention period for audit records generated by the information system; and |  |
| **AU-11.1.2** | 1. the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. |  |

|  |  |  |
| --- | --- | --- |
| **AU-12** | **AUDIT GENERATION** | **RESULTS** |
| **AU-12.1** | Determine if: |  |
| **AU-12.1.1** | 1. the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2; |  |
| **AU-12.1.2** | 1. the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2; |  |
| **AU-12.1.3** | 1. the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and |  |
| **AU-12.1.4** | 1. the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. |  |

### Security Assessment and Authorization (CA)

|  |  |  |
| --- | --- | --- |
| **CA-1** | **SECURITY ASSESSMENTS AND AUTHORIZATION POLICIES AND PROCEDURES** | **RESULTS** |
| **CA-1.1** | Determine if: |  |
| **CA-1.1.1** | 1. the organization develops and formally documents security assessment and authorization policy; |  |
| **CA-1.1.2** | 1. the organization security assessment and authorization policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **CA-1.1.3** | 1. the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities; |  |
| **CA-1.1.4** | 1. the organization develops and formally documents security assessment and authorization procedures; |  |
| **CA-1.1.5** | 1. the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and |  |
| **CA-1.1.6** | 1. the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities. |  |
| **CA-1.2** | Determine if: |  |
| **CA-1.2.1** | 1. the organization defines the frequency of security assessment and authorization policy reviews/updates; |  |
| **CA-1.2.2** | 1. the organization reviews/updates security assessment and authorization policy in accordance with organization-defined frequency; and |  |
| **CA-1.2.3** | 1. the organization defines the frequency of security assessment and authorization procedure reviews/updates; |  |
| **CA-1.2.4** | 1. the organization reviews/updates security assessment and authorization procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CA-2** | **SECURITY ASSESSMENTS** | **RESULTS** |
| **CA-2.1** | Determine if: |  |
| **CA-2.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of security control assessments and the frequency is at least annually; and |  |
| **CA-2.1.2** | 1. the organization conducts an assessment of the security controls in the information system at an organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CA-2(1)** | **SECURITY ASSESSMENTS – CONTROL ENHANCEMENT** | **RESULTS** |
| **CA-2.1(1)** | Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CA-3** | **INFORMATION SYSTEM CONNECTIONS** | **RESULTS** |
| **CA-3.1** | Determine if: |  |
| **CA-3.1.1** | 1. the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary); |  |
| **CA-3.1.2** | 1. the organization authorizes all connections from the information system to external information systems through the use of system connection agreements; and |  |
| **CA-3.1.3** | 1. the organization monitors/controls the system interconnections on an ongoing basis. |  |

|  |  |  |
| --- | --- | --- |
| **CA-5** | **PLAN OF ACTION AND MILESTONES** | **RESULTS** |
| **CA-5.1** | Determine if: |  |
| **CA-5.1.1** | 1. the organization develops a plan of action and milestones for the information system; |  |
| **CA-5.1.2** | 1. the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; |  |
| **CA-5.1.3** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates; and |  |
| **CA-5.1.4** | 1. the organization updates the plan of action and milestones at an organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CA-6** | **SECURITY AUTHORIZATION** | **RESULTS** |
| **CA-6.1** | Determine if: |  |
| **CA-6.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years; |  |
| **CA-6.1.2** | 1. the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization at an organization-defined frequency or when there is a significant change to the information system; |  |
| **CA-6.1.3** | 1. a senior organizational official signs and approves the security accreditation; and |  |
| **CA-6.1.4** | 1. the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37. |  |

|  |  |  |
| --- | --- | --- |
| **CA-7** | **CONTINUOUS MONITORING** | **RESULTS** |
| **CA-7.1** | Determine if: |  |
| **CA-7.1.1** | 1. the organization monitors the security controls in the information system on an ongoing basis; and |  |
| **CA-7.1.2** | 1. the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A. |  |
| **CA-7.2.1** | 1. the organization conducts security impact analyses on changes to the information system; |  |
| **CA-7.2.2** | 1. the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and |  |
| **CA-7.2.3** | 1. the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls. |  |

### Configuration Management (CM)

|  |  |  |
| --- | --- | --- |
| **CM-1** | **CONFIGURATION MANAGEMENT POLICY AND PROCEDURES** | **RESULTS** |
| **CM-1.1** | Determine if: |  |
| **CM-1.1.1** | 1. the organization develops and formally documents configuration management policy; |  |
| **CM-1.1.2** | 1. the organization configuration management policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **CM-1.1.3** | 1. the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities; |  |
| **CM-1.1.4** | 1. the organization develops and formally documents configuration management procedures; |  |
| **CM-1.1.5** | 1. the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls; and |  |
| **CM-1.1.6** | 1. the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities. |  |
| **CM-1.2** | Determine if: |  |
| **CM-1.2.1** | 1. the organization defines the frequency of configuration management policy reviews/updates; |  |
| **CM-1.2.2** | 1. the organization reviews/updates configuration management policy in accordance with organization-defined frequency; and |  |
| **CM-1.2.3** | 1. the organization defines the frequency of configuration management procedure reviews/updates; |  |
| **CM-1.2.4** | 1. the organization reviews/updates configuration management procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2** | **BASELINE CONFIGURATION** | **RESULTS** |
| **CM-2.1** | Determine if: |  |
| **CM-2.1.1** | 1. the organization develops and documents a baseline configuration of the information system that is consistent with the Federal Enterprise Architecture, shows relationships among information system components, and provides a well-defined and documented specification to which the information system is built; |  |
| **CM-2.1.2** | 1. the organization maintains the baseline configuration; and |  |
| **CM-2.1.3** | 1. the organization documents deviations from the baseline configuration, in support of mission needs/objectives. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2(1)** | **BASELINE CONFIGURATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-2(1).1** | Determine if the organization updates the baseline configuration of the information system as an integral part of information system component installations. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2(3)** | **BASELINE CONFIGURATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-2(3).1** | Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback. |  |

|  |  |  |
| --- | --- | --- |
| **CM-2(4)** | **BASELINE CONFIGURATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-2(4).1** | Determine if: |  |
| **CM-2(4).1.1** | 1. the organization develops and maintains a list of software programs not authorized to execute on the information system; and |  |
| **CM-2(4).1.2** | 1. the organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-3** | **CONFIGURATION CHANGE CONTROL** | **RESULTS** |
| **CM-3.1** | Determine if: |  |
| **CM-3.1.1** | 1. the organization authorizes, documents, and controls changes to the information system using an organizationally approved process; |  |
| **CM-3.1.2** | 1. the organization configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications; |  |
| **CM-3.1.3** | 1. the organization approves changes to the information system with consideration for the results from the security impact analysis of the change; and |  |
| **CM-3.1.4** | 1. the organization audits activities associated with configuration changes to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-3(2)** | **CONFIGURATION CHANGE CONTROL – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-3(2).1** | Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-4** | **SECURITY IMPACT ANALYSIS** | **RESULTS** |
| **CM-4.1** | Determine if the organization monitors changes to the information system by verifying that the organization:   * prior to change implementation and as part of the change approval process, conducts security impact analyses to assess the effects of the system changes; * after the system is changed (including upgrades and modifications), checks the security features to confirm that the features are still functioning properly; and * audits activities associated with configuration changes to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-5** | **ACCESS RESTRICTIONS FOR CHANGE** | **RESULTS** |
| **CM-5.1** | Determine if: |  |
| **CM-5.1.1** | 1. the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system, including upgrades, and modifications; and |  |
| **CM-5.1.2** | 1. the organization generates, retains, and reviews records reflecting all such changes to the information system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-6** | **CONFIGURATION SETTINGS** | **RESULTS** |
| **CM-6.1** | Determine if: |  |
| **CM-6.1.1** | 1. the organization establishes mandatory configuration settings for information technology products employed within the information system; |  |
| **CM-6.1.2** | 1. the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; |  |
| **CM-6.1.3** | 1. the organization documents the configuration settings; |  |
| **CM-6.1.4** | 1. the organization enforces the configuration settings in all components of the information system; and |  |
| **CM-6.1.5** | 1. the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. |  |

|  |  |  |
| --- | --- | --- |
| **CM-6(3)** | **CONFIGURATION SETTINGS – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-6(3).1** | Determine if: |  |
| **CM-6(3).1.1** | 1. the organization incorporates detection of unauthorized, security-relevant configuration changes into the organization’s incident response capability; and |  |
| **CM-6(3).1.2** | 1. the organization ensures that such detected events are tracked, monitored, corrected, and available for historical purposes. |  |

|  |  |  |
| --- | --- | --- |
| **CM-7** | **LEAST FUNCTIONALITY** | **RESULTS** |
| **CM-7.1** | Determine if: |  |
| **CM-7.1.1** | 1. the organization defines in the security plan, explicitly or by reference, prohibited or restricted functions, ports, protocols, and services for the information system; |  |
| **CM-7.1.2** | 1. the organization configures the information system to provide only essential capabilities; and |  |
| **CM-7.1.3** | 1. the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined functions, ports, protocols, and/or services. |  |

|  |  |  |
| --- | --- | --- |
| **CM-7(1)** | **LEAST FUNCTIONALITY – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-7(1).1** | Determine if: |  |
| **CM-7(1).1.1** | 1. the organization defines the frequency of information system reviews to identify and eliminate unnecessary: - functions; - ports; - protocols; and/or - services; and |  |
| **CM-7(1).1.2** | 1. the organization reviews the information system in accordance with organization-defined frequency to identify and eliminate unnecessary: - functions; - ports; - protocols; and/or - services. |  |

|  |  |  |
| --- | --- | --- |
| **CM-8** | **INFORMATION SYSTEM COMPONENT INVENTORY** | **RESULTS** |
| **CM-8.1** | Determine if: |  |
| **CM-8.1.1** | 1. the organization develops and documents an inventory of the components of the information system:  * that is at the level of granularity deemed appropriate by the organization for the components included in the inventory that are subject to tracking and reporting; * that includes any information determined to be necessary by the organization to achieve effective property accountability; and * that is consistent with the accreditation boundary of the system; and |  |
| **CM-8.1.2** | 1. the organization maintains the inventory of the components of the information system to reflect the current state of the system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-8(1)** | **INFORMATION SYSTEM COMPONENT INVENTORY – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-8(1).1** | Determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. |  |

|  |  |  |
| --- | --- | --- |
| **CM-8(5)** | **INFORMATION SYSTEM COMPONENT INVENTORY – CONTROL ENHANCEMENT** | **RESULTS** |
| **CM-8(5).1** | Determine if: |  |
| **CM-8(5).1.1** | 1. the organization updates the inventory of information system components as an integral part of component installations. |  |

|  |  |  |
| --- | --- | --- |
| **CM-9** | **CONFIGURATION MANAGEMENT PLAN** | **RESULTS** |
| **CM-9.1** | Determine if the organization develops, documents, and implements a configuration  management plan for the information system that:   * addresses roles, responsibilities, and configuration management processes and procedures; * defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and * establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items. |  |

### Contingency Planning (CP)

|  |  |  |
| --- | --- | --- |
| **CP-1** | **CONTINGENCY PLANNING POLICY AND PROCEDURES** | **RESULTS** |
| **CP-1.1** | Determine if: |  |
| **CP-1.1.1** | 1. the organization develops and formally documents contingency planning policy; |  |
| **CP-1.1.2** | 1. the organization contingency planning policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and compliance; |  |
| **CP-1.1.3** | 1. the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities; |  |
| **CP-1.1.4** | 1. the organization develops and formally documents contingency planning procedures; |  |
| **CP-1.1.5** | 1. the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls; and |  |
| **CP-1.1.6** | 1. the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities. |  |
| **CP-1.2** | Determine if: |  |
| **CP-1.2.1** | 1. the organization defines the frequency of contingency planning policy reviews/updates; |  |
| **CP-1.2.2** | 1. the organization reviews/updates contingency planning policy in accordance with organization-defined frequency; and |  |
| **CP-1.2.3** | 1. the organization defines the frequency of contingency planning procedure reviews/updates; |  |
| **CP-1.2.4** | 1. the organization reviews/updates contingency planning procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CP-2** | **CONTINGENCY PLAN** | **RESULTS** |
| **CP-2.1** | Determine if: |  |
| **CP-2.1.1** | 1. the organization and documents a contingency plan for the information system; |  |
| **CP-2.1.2** | 1. the contingency plan is consistent with NIST Special Publication 800-34; and |  |
| **CP-2.1.3** | 1. the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure; |  |
| **CP-2.1.4** | 1. the contingency plan is reviewed and approved by designated organizational officials; and |  |
| **CP-2.1.5** | 1. the organization disseminates the contingency plan to key contingency personnel. |  |

|  |  |  |
| --- | --- | --- |
| **CP-2(1)** | **CONTINGENCY PLAN – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-2(1).1** | Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan). |  |

|  |  |  |
| --- | --- | --- |
| **CP-3** | **CONTINGENCY TRAINING** | **RESULTS** |
| **CP-3.1** | Determine if: |  |
| **CP-3.1.1** | 1. the organization provides contingency training to personnel with contingency roles and responsibilities; |  |
| **CP-3.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually; and |  |
| **CP-3.1.3** | 1. the organization provides initial training and refresher training in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **CP-4** | **CONTINGENCY PLAN TESTING AND EXERCISES** | **RESULTS** |
| **CP-4.1** | Determine if: |  |
| **CP-4.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted; |  |
| **CP-4.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually; |  |
| **CP-4.1.3** | 1. the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; and |  |
| **CP-4.1.4** | 1. the organization reviews the contingency plan test/exercise results and takes corrective actions. |  |
| **CP-4.2.1** | 1. the contingency plan tests/exercises confirm the plan’s effectiveness; |  |
| **CP-4.2.2** | 1. the contingency plan tests/exercises confirm the organization’s readiness to execute the plan; and |  |
| **CP-4.2.3** | 1. the contingency plan tests/exercises confirm the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. |  |

|  |  |  |
| --- | --- | --- |
| **CP-4(1)** | **CONTINGENCY PLAN TESTING AND EXERCISES – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-4(1).1** | Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan). |  |

|  |  |  |
| --- | --- | --- |
| **CP-6** | **ALTERNATE STORAGE SITE** | **RESULTS** |
| **CP-6.1** | Determine if: |  |
| **CP-6.1.1** | 1. the organization identifies an alternate storage site; and |  |
| **CP-6.1.2** | 1. the organization initiates necessary alternate storage site agreements to permit storage of information system backup information. |  |

|  |  |  |
| --- | --- | --- |
| **CP-6(1)** | **ALTERNATE STORAGE SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-6(1).1** | Determine if: |  |
| **CP-6(1).1.1** | 1. the contingency plan or Contingency Planning Policy identifies the primary storage site hazards; and |  |
| **CP-6(1).1.2** | 1. the alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site. |  |

|  |  |  |
| --- | --- | --- |
| **CP-6(3)** | **ALTERNATE STORAGE SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-6(3).1** | Determine if: |  |
| **CP-6(3).1.1** | 1. the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and |  |
| **CP-6(3).1.2** | 1. the organization defines explicit mitigation actions for potential accessibility problems. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7** | **ALTERNATE PROCESSING SITE** | **RESULTS** |
| **CP-7.1** | Determine if: |  |
| **CP-7.1.1** | 1. the organization identifies an alternate processing site; |  |
| **CP-7.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the time period within which processing must be resumed at the alternate processing site; and |  |
| **CP-7.1.3** | 1. the organization initiates necessary alternate processing site agreements to permit the resumption of information system operations for critical mission/business functions within organization-defined time period. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(1)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(1).1** | Determine if: |  |
| **CP-7(1).1.1** | 1. the contingency plan identifies the primary processing site hazards; and |  |
| **CP-7(1).1.2** | 1. the alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(2)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(2).1** | Determine if: |  |
| **CP-7(2).1.1** | 1. the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and |  |
| **CP-7(2).1.2** | 1. the contingency plan defines explicit mitigation actions for potential accessibility problems. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(3)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(3).1** | Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization’s availability requirements. |  |

|  |  |  |
| --- | --- | --- |
| **CP-7(5)** | **ALTERNATE PROCESSING SITE – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-7(5).1** | Determine if the alternate processing site provides information security measures equivalent to that of the primary site. |  |

|  |  |  |
| --- | --- | --- |
| **CP-8** | **TELECOMMUNICATIONS SERVICES** | **RESULTS** |
| **CP-8.1** | Determine if: |  |
| **CP-8.1.1** | 1. the organization identifies primary and alternate telecommunications services to support the information system; |  |
| **CP-8.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the time period within which resumption of information system operations must take place; and |  |
| **CP-8.1.3** | 1. the organization initiates necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable. |  |
| **CP-8.2.1** | 1. the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness when the primary and/or alternate telecommunications services are provided by a common carrier. |  |

|  |  |  |
| --- | --- | --- |
| **CP-8(1)** | **TELECOMMUNICATIONS SERVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-8(1).1** | Determine if the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements. |  |

|  |  |  |
| --- | --- | --- |
| **CP-8(2)** | **TELECOMMUNICATIONS SERVICES – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-8(2).1** | Determine if the organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services. |  |

|  |  |  |
| --- | --- | --- |
| **CP-9** | **INFORMATION SYSTEM BACKUP** | **RESULTS** |
| **CP-9.1** | Determine if: |  |
| **CP-9.1.1** | 1. the organization defines the frequency of information systems backups; |  |
| **CP-9.1.2** | 1. the organization backs up user-level and system-level information (including system state information) in accordance with the organization-defined frequency; and |  |
| **CP-9.1.3** | 1. the organization backs up information to alternate storage sites (if so designated) at a frequency and transfer rate consistent with the organization’s recovery time objectives and recovery point objectives. |  |
| **CP-9.2.1** | 1. the organization protects backup information at the designated storage locations. |  |

|  |  |  |
| --- | --- | --- |
| **CP-9(1)** | **INFORMATION SYSTEM BACKUP – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-9(1).1** | Determine if: |  |
| **CP-9(1).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of information system backup testing; |  |
| **CP-9(1).1.2** | 1. the organization conducts information system backup testing in accordance with organization-defined frequency; and |  |
| **CP-9(1).1.3** | 1. testing results verify backup media reliability and information integrity. |  |

|  |  |  |
| --- | --- | --- |
| **CP-10** | **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION** | **RESULTS** |
| **CP-10.1** | Determine if the organization provides and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure. |  |

|  |  |  |
| --- | --- | --- |
| **CP-10(2)** | **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-10(2).1** | Determine if the information system implements transaction recovery for systems that are transaction-based. |  |

|  |  |  |
| --- | --- | --- |
| **CP-10(3)** | **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **CP-10(3).1** | Determine if: |  |
| **CP-10(3).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state; and |  |
| **CP-10(3).1.2** | 1. the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state. |  |

### Identification and Authentication (IA)

|  |  |  |
| --- | --- | --- |
| **IA-1** | **IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES** | **RESULTS** |
| **IA-1.1** | Determine if: |  |
| **IA-1.1.1** | 1. the organization develops and formally documents identification and authentication policy; |  |
| **IA-1.1.2** | 1. the organization identification and authentication policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **IA-1.1.3** | 1. the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities; |  |
| **IA-1.1.4** | 1. the organization develops and formally documents identification and authentication procedures; |  |
| **IA-1.1.5** | 1. the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls; and |  |
| **IA-1.1.6** | 1. the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities. |  |
| **IA-1.2** | Determine if: |  |
| **IA-1.2.1** | 1. the organization defines the frequency of identification and authentication policy reviews/updates; |  |
| **IA-1.2.2** | 1. the organization reviews/updates identification and authentication policy in accordance with organization-defined frequency; and |  |
| **IA-1.2.3** | 1. the organization defines the frequency of identification and authentication procedure reviews/updates; |  |
| **IA-1.2.4** | 1. the organization reviews/updates identification and authentication procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)** | **RESULTS** |
| **IA-2.1** | Determine if: |  |
| **IA-2.1.1** | 1. The information system uniquely identifies and authenticates users (or processes acting on behalf of users); and |  |
| **IA-2.1.2** | 1. Authentication levels for users (or processes acting on behalf of users) are consistent with NIST Special Publication 800-63 and e-authentication risk assessment results. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(1)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(1).1** | Determine if: |  |
| **IA-2(1).1.1** | 1. the organization defines in the security plan, explicitly or by reference, the NIST Special Publication 800-63 authentication levels for the information system; and |  |
| **IA-2(1).1.2** | 1. the information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3, level 3 using a hardware authentication device or level 4. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(2)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(2).1** | Determine if the information system uses multifactor authentication for network access to non-privileged accounts. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(3)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(3).1** | Determine if the information system uses multifactor authentication for local access to privileged accounts. |  |

|  |  |  |
| --- | --- | --- |
| **IA-2(8)** | **USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-2(8).1** | Determine if: |  |
| **IA-2(8).1.1** | 1. the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and |  |
| **IA-2(8).1.2** | 1. the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts. |  |

|  |  |  |
| --- | --- | --- |
| **IA-3** | **DEVICE IDENTIFICATION AND AUTHENTICATION** | **RESULTS** |
| **IA-3.1** | Determine if: |  |
| **IA-3.1.1** | 1. the organization defines the devices for which identification and authentication is required before establishing connections to the information system; |  |
| **IA-3.1.2** | 1. the information system uniquely identifies and authenticates the devices defined by the organization before establishing connections to the information system; and |  |
| **IA-3.1.3** | 1. the information system employs device authentication mechanisms with strength of mechanism determined by the FIPS 199 security categorization of the information system. |  |

|  |  |  |
| --- | --- | --- |
| **IA-4** | **IDENTIFIER MANAGEMENT** | **RESULTS** |
| **IA-4.1** | Determine if: |  |
| **IA-4.1.1** | 1. the organization manages user identifiers by uniquely identifying each user; |  |
| **IA-4.1.2** | 1. the organization manages user identifiers by verifying the identity of each user; |  |
| **IA-4.1.3** | 1. the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official; |  |
| **IA-4.1.4** | 1. the organization manages user identifiers by issuing the identifier to the intended party; |  |
| **IA-4.1.5** | 1. the organization defines in the security plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled; |  |
| **IA-4.1.6** | 1. the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and |  |
| **IA-4.1.7** | 1. the organization manages user identifiers by archiving identifiers. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5** | **AUTHENTICATOR MANAGEMENT** | **RESULTS** |
| **IA-5.1** | Determine if: |  |
| **IA-5.1.1** | 1. the organization defines the time period (by authenticator type) for changing/refreshing authenticators; and |  |
| **IA-5.1.2** | 1. the organization manages information system authenticators for users and devices by:  * verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; * establishing initial authenticator content for authenticators defined by the organization; * ensuring that authenticators have sufficient strength of mechanism for their intended use; * establishing and implementing administrative procedures for initial authenticator distribution; * establishing and implementing administrative procedures for lost/compromised or damaged authenticators; * establishing and implementing administrative procedures for revoking authenticators; * changing default content of authenticators upon information system installation; * establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization); * changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type; * protecting authenticator content from unauthorized disclosure and modification; and * requiring users to take, and having devices implement, specific measures to safeguard authenticators. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5(1)** | **AUTHENTICATOR MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-5(1).1** | Determine if: |  |
| **IA-5(1).1.1** | 1. the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower case letters, numbers, and special characters including minimum requirements for each type; |  |
| **IA-5(1).1.2** | 1. the organization defines the minimum number of characters that must be changed when new passwords are created; |  |
| **IA-5(1).1.3** | 1. the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters; |  |
| **IA-5(1).1.4** | 1. the organization defines the number of generations for which password reuse is prohibited; and |  |
| **IA-5(1).1.5** | 1. the information system, for password-based authentication:  * enforces the minimum password complexity standards that meet the organization-defined requirements; * enforces the organization-defined minimum number of characters that must be changed when new passwords are created; * encrypts passwords in storage and in transmission; * enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and * prohibits password reuse for the organization-defined number of generations. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5(2)** | **AUTHENTICATOR MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-5(2).1** | Determine if the information system, for PKI-based authentication:   * validates certificates by constructing a certification path with status information with an accepted trust anchor; * enforces authorized access to the corresponding private key; and * maps the authenticated identity to the user account. |  |

|  |  |  |
| --- | --- | --- |
| **IA-5(3)** | **AUTHENTICATOR MANAGEMENT – CONTROL ENHANCEMENT** | **RESULTS** |
| **IA-5(3).1** | Determine if: |  |
| **IA-5(3).1.1** | 1. the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official; and |  |
| **IA-5(3).1.2** | 1. the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). |  |

|  |  |  |
| --- | --- | --- |
| **IA-6** | **AUTHENTICATOR FEEDBACK** | **RESULTS** |
| **IA-6.1** | Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. |  |

|  |  |  |
| --- | --- | --- |
| **IA-7** | **CRYPTOGRAPHIC MODULE AUTHENTICATION** | **RESULTS** |
| **IA-7.1** | Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Order, directive, policies, regulation, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended). |  |

|  |  |  |
| --- | --- | --- |
| **IA-8** | **IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)** | **RESULTS** |
| **IA-8.1** | Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). |  |

### Incident Response (IR)

|  |  |  |
| --- | --- | --- |
| **IR-1** | **INCIDENT RESPONSE POLICY AND PROCEDURES** | **RESULTS** |
| **IR-1.1** | Determine if: |  |
| **IR-1.1.1** | 1. the organization develops and formally documents incident response policy; |  |
| **IR-1.1.2** | 1. the organization incident response policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **IR-1.1.3** | 1. the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities; |  |
| **IR-1.1.4** | 1. the organization develops and formally documents incident response procedures; |  |
| **IR-1.1.5** | 1. the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls; and |  |
| **IR-1.1.6** | 1. the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities. |  |
| **IR-1.2** | Determine if: |  |
| **IR-1.2.1** | 1. the organization defines the frequency of incident response policy reviews/updates; |  |
| **IR-1.2.2** | 1. the organization reviews/updates incident response policy in accordance with organization-defined frequency; and |  |
| **IR-1.2.3** | 1. the organization defines the frequency of incident response procedure reviews/updates; |  |
| **IR-1.2.4** | 1. the organization reviews/updates incident response procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **IR-2** | **INCIDENT RESPONSE TRAINING** | **RESULTS** |
| **IR-2.1** | Determine if: |  |
| **IR-2.1.1** | 1. The organization identifies and documents personnel with incident response roles and responsibilities; |  |
| **IR-2.1.2** | 1. The organization provides incident response training to personnel with incident response roles and responsibilities; |  |
| **IR-2.1.2** | 1. Incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities; |  |
| **IR-2.1.2** | 1. The organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually; and |  |
| **IR-2.1.2** | 1. The organization provides refresher incident response training in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **IR-3** | **INCIDENT RESPONSE TESTING AND EXERCISES** | **RESULTS** |
| **IR-3.1** | Determine if: |  |
| **IR-3.1.1** | 1. the organization defines in the security plan, explicitly or by reference, incident response test/exercises; |  |
| **IR-3.1.2** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of incident response test/exercises and the frequency is at least annually; |  |
| **IR-3.1.3** | 1. the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization defined frequency; |  |
| **IR-3.1.4** | 1. the organization documents the results of incident response test/exercises; and |  |
| **IR-3.1.5** | 1. the organization determines the effectiveness of the incident response capability. |  |

|  |  |  |
| --- | --- | --- |
| **IR-4** | **INCIDENT HANDLING** | **RESULTS** |
| **IR-4.1** | Determine if: |  |
| **IR-4.1.1** | 1. the organization implements and incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and |  |
| **IR-4.1.2** | 1. the organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. |  |

|  |  |  |
| --- | --- | --- |
| **IR-4(1)** | **INCIDENT HANDLING – CONTROL ENHANCEMENT** | **RESULTS** |
| **IR-4(1).1** | Determine if the organization employs automated mechanisms to support the incident handling process. |  |

|  |  |  |
| --- | --- | --- |
| **IR-5** | **INCIDENT MONITORING** | **RESULTS** |
| **IR-5.1** | Determine if the organization tracks and documents information system security incidents on an ongoing basis. |  |

|  |  |  |
| --- | --- | --- |
| **IR-6** | **INCIDENT REPORTING** | **RESULTS** |
| **IR-6.1** | Determine if: |  |
| **IR-6.1.1** | 1. the organization promptly reports incident information to appropriate authorities; |  |
| **IR-6.1.2** | 1. incident reporting is consistent with NIST Special Publication 800-61; |  |
| **IR-6.1.3** | 1. the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and |  |
| **IR-6.1.4** | 1. weakness and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. |  |

|  |  |  |
| --- | --- | --- |
| **IR-6(1)** | **INCIDENT REPORTING – CONTROL ENHANCEMENT** | **RESULTS** |
| **IR-6(1).1** | Determine if the organization employs automated mechanisms to assist in the reporting of security incidents. |  |

|  |  |  |
| --- | --- | --- |
| **IR-7** | **INCIDENT RESPONSE ASSISTANCE** | **RESULTS** |
| **IR-7.1** | Determine if: |  |
| **IR-7.1.1** | 1. the organization provides and incident response support resource that offers advice and assistance to user of the information system for the handling and reporting of security incidents; and |  |
| **IR-7.1.2** | 1. the incident response support resources is an integral parts of the organization’s incident response capability. |  |

|  |  |  |
| --- | --- | --- |
| **IR-7(1)** | **INCIDENT RESPONSE ASSISTANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **IR-7(1).1** | Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support. |  |

|  |  |  |
| --- | --- | --- |
| **IR-8** | **INCIDENT RESPONSE PLAN** | **RESULTS** |
| **IR-8.1** | Determine if: |  |
| **IR-8.1.1** | 1. the organization develops an incident response plan that:   - provides the organization with a roadmap for implementing its incident response  capability;  - describes the structure and organization of the incident response capability;  - provides a high-level approach for how the incident response capability fits into the  overall organization;  - meets the unique requirements of the organization, which relate to mission, size,  structure, and functions;  - defines reportable incidents;  - provides metrics for measuring the incident response capability within the organization;  - defines the resources and management support needed to effectively maintain and mature an incident response capability; and  - is reviewed and approved by designated officials within the organization. |  |
| **IR-8.1.2** | 1. the organization defines, in the incident response plan, incident response personnel   (identified by name and/or role) and organizational elements;  (ii) the organization distributes copies of the incident response plan to incident  response personnel and organizational elements identified in the plan;  (iii) the organization defines, in the incident response plan, the frequency to review the  plan;  (iv) the organization reviews the incident response plan in accordance with the  organization-defined frequency;  (v) the organization revises the incident response plan to address system/organizational  changes or problems encountered during plan implementation, execution, or  testing; and  (vi) the organization communicates incident response plan changes to incident response  personnel and organizational elements identified in the plan. |  |

### Maintenance (MA)

|  |  |  |
| --- | --- | --- |
| **MA-1** | **SYSTEM MAINTENANCE POLICY AND PROCEDURES** | **RESULTS** |
| **MA-1.1** | Determine if: |  |
| **MA-1.1.1** | 1. the organization develops and formally documents system maintenance policy; |  |
| **MA-1.1.2** | 1. the organization system maintenance policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **MA-1.1.3** | 1. the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities; |  |
| **MA-1.1.4** | 1. the organization develops and formally documents system maintenance procedures; |  |
| **MA-1.1.5** | 1. the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls; and |  |
| **MA-1.1.6** | 1. the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities. |  |
| **MA-1.2** | Determine if: |  |
| **MA-1.2.1** | 1. the organization defines the frequency of system maintenance policy reviews/updates; |  |
| **MA-1.2.2** | 1. the organization reviews/updates system maintenance policy in accordance with organization-defined frequency; and |  |
| **MA-1.2.3** | 1. the organization defines the frequency of system maintenance procedure reviews/updates; |  |
| **MA-1.2.4** | 1. the organization reviews/updates system maintenance procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **MA-2** | **CONTROLLED MAINTENANCE** | **RESULTS** |
| **MA-2.1** | Determine if: |  |
| **MA-2.1.1** | 1. the organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; |  |
| **MA-2.1.2** | 1. the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; |  |
| **MA-2.1.3** | 1. the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for offsite maintenance or repairs; |  |
| **MA-2.1.4** | 1. the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and |  |
| **MA-2.1.5** | 1. the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. |  |

|  |  |  |
| --- | --- | --- |
| **MA-2(1)** | **CONTROLLED MAINTENANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-2(1).1** | Determine if the organization maintains maintenance records for the information system  that include:   * date and time of maintenance; * name of the individual performing the maintenance; * name of escort, if necessary; * a description of the maintenance performed; and * a list of equipment removed or replaced (including identification numbers, if applicable). |  |

|  |  |  |
| --- | --- | --- |
| **MA-3** | **MAINTENANCE TOOLS** | **RESULTS** |
| **MA-3.1** | Determine if: |  |
| **MA-3.1.1** | 1. the organization approves, controls, and monitors the use of information system maintenance tools; and |  |
| **MA-3.1.2** | 1. the organization maintains maintenance tools on an ongoing basis. |  |

|  |  |  |
| --- | --- | --- |
| **MA-3(1)** | **MAINTENANCE TOOLS – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-3(1).1** | Determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. |  |

|  |  |  |
| --- | --- | --- |
| **MA-3(2)** | **MAINTENANCE TOOLS – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-3(2).1** | Determine if the organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system. |  |

|  |  |  |
| --- | --- | --- |
| **MA-4** | **NON-LOCAL MAINTENANCE** | **RESULTS** |
| **MA-4.1** | Determine if: |  |
| **MA-4.1.1** | 1. the organization authorizes, monitors, and controls the executions of maintenance and diagnostic activities conducted remotely by individuals communication through an external, non-organization-controlled network (e.g., the internet) , if employed; |  |
| **MA-4.1.2** | 1. the organization documents in the security plan, the remote maintenance and diagnostic tools to be employed; |  |
| **MA-4.1.3** | 1. the organization maintains records for all remote maintenance and diagnostic activities; |  |
| **MA-4.1.4** | 1. the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of remote maintenance and diagnostic activity when the remote maintenance or diagnostics is completed.; and |  |
| **MA-4.1.5** | 1. the organization changes the passwords following each remote maintenance and diagnostic activity if password-based authentication is used to accomplish remote maintenance. |  |

|  |  |  |
| --- | --- | --- |
| **MA-4(1)** | **NON-LOCAL MAINTENANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-4(1).1** | Determine if: |  |
| **MA-4(1).1.1** | 1. the organization audits non-local maintenance and diagnostic sessions; and |  |
| **MA-4(1).1.2** | 1. designated organizational personnel review the maintenance records of the sessions. |  |

|  |  |  |
| --- | --- | --- |
| **MA-4(2)** | **NON-LOCAL MAINTENANCE – CONTROL ENHANCEMENT** | **RESULTS** |
| **MA-4(2).1** | Determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system. |  |

|  |  |  |
| --- | --- | --- |
| **MA-5** | **MAINTENANCE PERSONNEL** | **RESULTS** |
| **MA-5.1** | Determine if: |  |
| **MA-5.1.1** | 1. the organization allows only authorized personnel to perform maintenance on the information system; and |  |
| **MA-5.1.2** | 1. the organization supervises authorized maintenance personnel who do not have needed access authorizations to the information system during the performance of maintenance activities on the system using organizational personnel with appropriate access authorizations. |  |

|  |  |  |
| --- | --- | --- |
| **MA-6** | **TIMELY MAINTENANCE** | **RESULTS** |
| **MA-6.1** | Determine if: |  |
| **MA-6.1.1** | 1. the organization defines in the security plan, explicitly or by reference, key information system components; |  |
| **MA-6.2.1** | 1. the organization defines in the security plan, explicitly or by reference, the time period within which support and spare parts mush be obtained after a failure; and |  |
| **MA-6.3.1** | 1. the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure. |  |

### Media Protection (MP)

|  |  |  |
| --- | --- | --- |
| **MP-1** | **MEDIA PROTECTION POLICY AND PROCEDURES** | **RESULTS** |
| **MP-1.1** | Determine if: |  |
| **MP-1.1.1** | 1. the organization develops and formally documents media protection policy; |  |
| **MP-1.1.2** | 1. the organization media protection policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **MP-1.1.3** | 1. the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities; |  |
| **MP-1.1.4** | 1. the organization develops and formally documents media protection procedures; |  |
| **MP-1.1.5** | 1. the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls; and |  |
| **MP-1.1.6** | 1. the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities. |  |
| **MP-1.2** | Determine if: |  |
| **MP-1.2.1** | 1. the organization defines the frequency of media protection policy reviews/updates; |  |
| **MP-1.2.2** | 1. the organization reviews/updates media protection policy in accordance with organization-defined frequency; and |  |
| **MP-1.2.3** | 1. the organization defines the frequency of media protection procedure reviews/updates; |  |
| **MP-1.2.4** | 1. the organization reviews/updates media protection procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **MP-2** | **MEDIA ACCESS** | **RESULTS** |
| **MP-2.1** | Determine if the organization restricts access to information system media to authorized users. |  |

|  |  |  |
| --- | --- | --- |
| **MP-2(1)** | **MEDIA ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **MP-2(1).1** | Determine if: |  |
| **MP-2(1).1.1** | 1. the organization employs automated mechanisms to restrict access to media storage areas; and |  |
| **MP-2(1).1.2** | 1. the organization employs automated mechanisms to audit access attempts and access granted. |  |

|  |  |  |
| --- | --- | --- |
| **MP-3** | **MEDIA MARKING** | **RESULTS** |
| **MP-3.1** | Determine if the organization: |  |
| **MP-3.1.1** | 1. defines removable media types and information system output that require marking; |  |
| **MP-3.1.2** | 1. marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; |  |
| **MP-3.1.3** | 1. defines:  * removable media types and information system output exempt from marking; * controlled areas designated for retaining removable media and information output exempt from marking; and |  |
| **MP-3.1.4** | 1. removable media and information system output exempt from marking remain within designated controlled areas. |  |

|  |  |  |
| --- | --- | --- |
| **MP-4** | **MEDIA STORAGE** | **RESULTS** |
| **MP-4.1** | Determine if: |  |
| **MP-4.1.1** | 1. the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk; |  |
| **MP-4.1.2** | 1. the organization defines the specific measures used to protect the selected media and information contained on that media; |  |
| **MP-4.1.3** | 1. the organization physically controls and securely stores information system media within controlled areas; and |  |
| **MP-4.1.4** | 1. the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media. |  |

|  |  |  |
| --- | --- | --- |
| **MP-5** | **MEDIA TRANSPORT** | **RESULTS** |
| **MP-5.1** | Determine if: |  |
| **MP-5.1.1** | 1. the organization identifies personnel authorized to transport information system media outside of controlled area; |  |
| **MP-5.1.2** | 1. the organization documents, in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media; |  |
| **MP-5.1.3** | 1. the organization protects and controls information system media during transport outside of controlled areas; and |  |
| **MP-5.1.4** | 1. the organization restricts the activities associated with transport of information system media to authorized personnel. |  |

|  |  |  |
| --- | --- | --- |
| **MP-5(2)** | **MEDIA TRANSPORT – CONTROL ENHANCEMENT** | **RESULTS** |
| **MP-5(2).1** | Determine if the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records. |  |

|  |  |  |
| --- | --- | --- |
| **MP-5(4)** | **MEDIA TRANSPORT – CONTROL ENHANCEMENT** | **RESULTS** |
| **MP-5(4).1** | Determine if the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. |  |

|  |  |  |
| --- | --- | --- |
| **MP-6** | **MEDIA SANITIZATION** | **RESULTS** |
| **MP-6.1** | Determine if: |  |
| **MP-6.1.1** | 1. the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in t process; |  |
| **MP-6.1.2** | 1. the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and |  |
| **MP-6.1.3** | 1. information system media sanitation is consistent with NIST Special Publication 800-88. |  |

### Physical and Environmental Protection (PE)

|  |  |  |
| --- | --- | --- |
| **PE-1** | **PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES** | **RESULTS** |
| **PE-1.1** | Determine if: |  |
| **PE-1.1.1** | 1. the organization develops and formally documents physical and environmental protection policy; |  |
| **PE-1.1.2** | 1. the organization physical and environmental protection policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **PE-1.1.3** | 1. the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities; |  |
| **PE-1.1.4** | 1. the organization develops and formally documents physical and environmental protection procedures; |  |
| **PE-1.1.5** | 1. the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and |  |
| **PE-1.1.6** | 1. the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities. |  |
| **PE-1.2** | Determine if: |  |
| **PE-1.2.1** | 1. the organization defines the frequency of physical and environmental protection policy reviews/updates; |  |
| **PE-1.2.2** | 1. the organization reviews/updates physical and environmental protection policy in accordance with organization-defined frequency; and |  |
| **PE-1.2.3** | 1. the organization defines the frequency of physical and environmental protection procedure reviews/updates; |  |
| **PE-1.2.4** | 1. the organization reviews/updates physical and environmental protection procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PE-2** | **PHYSICAL ACCESS AUTHORIZATIONS** | **RESULTS** |
| **PE-2.1** | Determine if: |  |
| **PE-2.1.1** | 1. the organization identifies areas within the facility that are publicly accessible; |  |
| **PE-2.1.2** | 1. the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and |  |
| **PE-2.1.3** | 1. the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). |  |
| **PE-2.2** | Determine if: |  |
| **PE-2.2.1** | 1. the organization defines the frequency for review and approval of the physical access list and authorization credentials for the facility; |  |
| **PE-2.2.2** | 1. organization reviews and approves the access list and authorization credentials in accordance with the organization-defined frequency; and |  |
| **PE-2.2.3** | 1. the organization removes from the access list personnel no longer requiring access. |  |

|  |  |  |
| --- | --- | --- |
| **PE-3.1** | Determine if: | **RESULTS** |
| **PE-3.1.1** | 1. the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); |  |
| **PE-3.1.2** | 1. the organization verifies individual access authorizations before granting access to the facility; |  |
| **PE-3.1.3** | 1. the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards; |  |
| **PE-3.1.4** | 1. the organization controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk; and |  |
| **PE-3.1.5** | 1. the organization secures keys, combinations, and other physical access devices. |  |

|  |  |  |
| --- | --- | --- |
| **PE-4** | **ACCESS CONTROL FOR TRANSMISSION MEDIUM** | **RESULTS** |
| **PE-4.1** | Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities. |  |

|  |  |  |
| --- | --- | --- |
| **PE-5** | **ACCESS CONTROL FOR DISPLAY MEDIUM** | **RESULTS** |
| **PE-5.1** | Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output. |  |

|  |  |  |
| --- | --- | --- |
| **PE-6** | **MONITORING PHYSICAL ACCESS** | **RESULTS** |
| **PE-6.1** | Determine if: |  |
| **PE-6.1.1** | 1. the organization monitors physical access to the information system to detect and respond to physical security incidents; |  |
| **PE-6.1.2** | 1. the organization defines the frequency to review physical access logs; |  |
| **PE-6.1.3** | 1. the organization reviews physical access logs in accordance with the organization-defined frequency; and |  |
| **PE-6.1.4** | 1. the organization coordinates results of reviews and investigations with the organization’s incident response capability. |  |

|  |  |  |
| --- | --- | --- |
| **PE-6(1)** | **MONITORING PHYSICAL ACCESS – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-6(1).1** | Determine if the organization monitors real-time intrusion alarms and surveillance equipment. |  |

|  |  |  |
| --- | --- | --- |
| **PE-7** | **VISITOR CONTROL** | **RESULTS** |
| **PE-7.1** | Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other that areas designated a publicly accessible. |  |

|  |  |  |
| --- | --- | --- |
| **PE-7(1)** | **VISITOR CONTROL – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-7(1).1** | Determine if the organization escorts visitors and monitors visitor activity, when required. |  |

|  |  |  |
| --- | --- | --- |
| **PE-8** | **ACCESS RECORDS** | **RESULTS** |
| **PE-8.1** | Determine if: |  |
| **PE-8.1.1** | 1. the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); |  |
| **PE-8.1.2** | 1. the organization defines the frequency to review visitor access records; |  |
| **PE-8.1.3** | 1. the organization reviews the visitor access records in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PE-9** | **POWER EQUIPMENT AND POWER CABLING** | **RESULTS** |
| **PE-9.1** | Determine if the organization protects power equipment and power cabling for the information system from damage and destruction. |  |

|  |  |  |
| --- | --- | --- |
| **PE-10** | **EMERGENCY SHUTOFF** | **RESULTS** |
| **PE-10.1** | Determine if: |  |
| **PE-10.1.1** | 1. the organization provides the capability of shutting off power to the information system or individual system components in emergency situations; |  |
| **PE-10.1.2** | 1. the organization defines the location of emergency shutoff switches or devices by information system or system component; |  |
| **PE-10.1.3** | 1. the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel; and |  |
| **PE-10.1.4** | 1. the organization protects the emergency power shutoff capability from unauthorized activation. |  |

|  |  |  |
| --- | --- | --- |
| **PE-11** | **EMERGENCY POWER** | **RESULTS** |
| **PE-11.1** | Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. |  |

|  |  |  |
| --- | --- | --- |
| **PE-12** | **EMERGENCY LIGHTING** | **RESULTS** |
| **PE-12.1** | Determine if: |  |
| **PE-12.1.1** | 1. the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption; |  |
| **PE-12.1.2** | 1. the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility; and |  |
| **PE-12.1.3** | 1. the organization maintains the automatic emergency lighting for the information system. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13** | **FIRE PROTECTION** | **RESULTS** |
| **PE-13.1** | Determine if: |  |
| **PE-13.1.1** | 1. the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source; and |  |
| **PE-13.1.2** | 1. the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13(1)** | **FIRE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-13(1).1** | Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13(2)** | **FIRE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-13(2).1** | Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. |  |

|  |  |  |
| --- | --- | --- |
| **PE-13(3)** | **FIRE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **PE-13(3).1** | Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis. |  |

|  |  |  |
| --- | --- | --- |
| **PE-14** | **TEMPERATURE AND HUMIDITY CONTROLS** | **RESULTS** |
| **PE-14.1** | Determine if: |  |
| **PE-14.1.1** | 1. the organization defines the acceptable temperature and humidity levels within the facility where the information system resides; |  |
| **PE-14.1.2** | 1. the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels; |  |
| **PE-14.1.3** | 1. the organization defines the frequency to monitor temperature and humidity levels; and |  |
| **PE-14.1.4** | 1. the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PE-15** | **WATER DAMAGE PROTECTION** | **RESULTS** |
| **PE-15.1** | Determine if: |  |
| **PE-15.1.1** | 1. the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly; and |  |
| **PE-15.1.2** | 1. key personnel within the organization have knowledge of the master water shutoff valves. |  |

|  |  |  |
| --- | --- | --- |
| **PE-16** | **DELIVERY AND REMOVAL** | **RESULTS** |
| **PE-16.1** | Determine if: |  |
| **PE-16.1.1** | 1. the organization defines the types of information system components to be authorized, monitored, and controlled as such components are entering or exiting the facility; |  |
| **PE-16.1.2** | 1. the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility; and |  |
| **PE-16.1.3** | 1. the organization maintains records of information system components entering and exiting the facility. |  |

|  |  |  |
| --- | --- | --- |
| **PE-17** | **ALTERNATE WORK SITE** | **RESULTS** |
| **PE-17.1** | Determine if: |  |
| **PE-17.1.1** | 1. the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites; |  |
| **PE-17.1.2** | 1. the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites; |  |
| **PE-17.1.3** | 1. the organization assesses, as feasible, the effectiveness of security controls at alternate work sites; and |  |
| **PE-17.1.4** | 1. the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems. |  |

|  |  |  |
| --- | --- | --- |
| **PE-18** | **LOCATION OF INFORMATION SYSTEM COMPONENTS** | **RESULTS** |
| **PE-18.1** | Determine if: |  |
| **PE-18.1.1** | 1. the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and |  |
| **PE-18.2.1** | 1. the organization positions information system components within the facility to minimize the opportunity for unauthorized access. |  |

### Planning (PL)

|  |  |  |
| --- | --- | --- |
| **PL-1** | **SECURITY PLANNING POLICY AND PROCEDURES** | **RESULTS** |
| **PL-1.1** | Determine if: |  |
| **PL-1.1.1** | 1. the organization develops and formally documents security planning policy; |  |
| **PL-1.1.2** | 1. the organization security planning policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **PL-1.1.3** | 1. the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities; |  |
| **PL-1.1.4** | 1. the organization develops and formally documents security planning procedures; |  |
| **PL-1.1.5** | 1. the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls; and |  |
| **PL-1.1.6** | 1. the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities. |  |
| **PL-1.2** | Determine if: |  |
| **PL-1.2.1** | 1. the organization defines the frequency of security planning policy reviews/updates; |  |
| **PL-1.2.2** | 1. the organization reviews/updates security planning policy in accordance with organization-defined frequency; and |  |
| **PL-1.2.3** | 1. the organization defines the frequency of security planning procedure reviews/updates; |  |
| **PL-1.2.4** | 1. the organization reviews/updates security planning procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PL-2** | **SYSTEM SECURITY PLAN** | **RESULTS** |
| **PL-2.1** | Determine if: |  |
| **PL-2.1.1** | 1. the organization develops and implements a security plan for the information system; |  |
| **PL-2.1.2** | 1. the security plan provides and overview of the security requirements for the information system and a description of the security controls planned r in place for meeting the security requirements; |  |
| **PL-2.1.3** | 1. the organizations defines in the security plan, explicitly or by reference, the values for all organization-defined parameters (i.e., assignment and selection operations) in applicable security controls and control enhancements; |  |
| **PL-2.1.4** | 1. the security plan development is consistent with NIST Special Publication 800-18; |  |
| **PL-2.1.5** | 1. the security plan is consistent with the organization’s information system architecture and information security architecture; and |  |
| **PL-2.1.6** | 1. designated organizational officials review and approve the security plan. |  |

|  |  |  |
| --- | --- | --- |
| **PL-4** | **RULES OF BEHAVIOR** | **RESULTS** |
| **PL-4.1** | Determine if: |  |
| **PL-4.1.1** | 1. the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information and information system usage; |  |
| **PL-4.2.1** | 1. the organization makes the rules available to all information system users; |  |
| **PL-4.3.1** | 1. the rules of behavior for organizational personnel are consistent with NIST Special Publication 800-18; and |  |
| **PL-4.4.1** | 1. the organization receives a signed acknowledgement from user’s indication that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information. |  |

|  |  |  |
| --- | --- | --- |
| **PL-5** | **PRIVACY IMPACT ASSESSMENT** | **RESULTS** |
| **PL-5.1** | Determine if: |  |
| **PL-5.1.1** | 1. the organization conducts a privacy impact assessment on the information system; and |  |
| **PL-5.1.2** | 1. the privacy impact assessment is compliant with OMB policy. |  |

|  |  |  |
| --- | --- | --- |
| **PL-6** | **SECURITY-RELATED ACTIVITY PLANNING** | **RESULTS** |
| **PL-6.1** | Determine if: |  |
| **PL-6.1.1** | 1. the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals; and |  |
| **PL-6.2.1** | 1. the organization’s advance planning and coordination of security-related activities includes both emergency and non-emergency situations. |  |

### Personnel Security (PS)

|  |  |  |
| --- | --- | --- |
| **PS-1** | **PERSONNEL SECURITY POLICY AND PROCEDURES** | **RESULTS** |
| **PS-1.1** | Determine if: |  |
| **PS-1.1.1** | 1. the organization develops and formally documents personnel security policy; |  |
| **PS-1.1.2** | 1. the organization personnel security policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **PS-1.1.3** | 1. the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities; |  |
| **PS-1.1.4** | 1. the organization develops and formally documents personnel security procedures; |  |
| **PS-1.1.5** | 1. the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls; and |  |
| **PS-1.1.6** | 1. the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities. |  |
| **PS-1.2** | Determine if: |  |
| **PS-1.2.1** | 1. the organization defines the frequency of personnel security policy reviews/updates; |  |
| **PS-1.2.2** | 1. the organization reviews/updates personnel security policy in accordance with organization-defined frequency; and |  |
| **PS-1.2.3** | 1. the organization defines the frequency of personnel security procedure reviews/updates; |  |
| **PS-1.2.4** | 1. the organization reviews/updates personnel security procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PS-2** | **POSITION CATEGORIZATION** | **RESULTS** |
| **PS-2.1** | Determine if: |  |
| **PS-2.1.1** | 1. the organization assigns a risk designations to all positions within the organization; |  |
| **PS-2.1.2** | 1. the organization establishes a screening criteria for individuals filling organizational positions; |  |
| **PS-2.1.3** | 1. the risk designations for the organizational positions are consistent with 5 CFR 731.106(a) and OPM policy and guidance; |  |
| **PS-2.1.4** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions; and |  |
| **PS-2.1.5** | 1. the organization reviews and revises position risk designations in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PS-3** | **PERSONNEL SCREENING** | **RESULTS** |
| **PS-3.1** | Determine if: |  |
| **PS-3.1.1** | 1. the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and |  |
| **PS-3.1.2** | 1. the personnel screening is consistent with 5 CFR 731.106, OPM policy, regulations, and guidance, FIPS 201 and NIST Special publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position. |  |

|  |  |  |
| --- | --- | --- |
| **PS-4** | **PERSONNEL TERMINATION** | **RESULTS** |
| **PS-4.1** | Determine if: |  |
| **PS-4.1.1** | 1. the organization terminates information system access upon termination of individual employment; |  |
| **PS-4.2.1** | 1. the organization conducts exit interviews of terminated personnel; |  |
| **PS-4.3.1** | 1. the organization retrieves all organizational information system-related property from terminated personnel; and |  |
| **PS-4.4.1** | 1. the organization retains access to official documents and records on organizational information systems created by terminated personnel. |  |

|  |  |  |
| --- | --- | --- |
| **PS-5** | **PERSONNEL TRANSFER** | **RESULTS** |
| **PS-5.1** | Determine if: |  |
| **PS-5.1.1** | 1. the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and |  |
| **PS-5.1.2** | 1. the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization. |  |

|  |  |  |
| --- | --- | --- |
| **PS-6** | **ACCESS AGREEMENTS** | **RESULTS** |
| **PS-6.1** | Determine if: |  |
| **PS-6.1.1** | 1. the organization requires appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access; |  |
| **PS-6.2.1** | 1. the organization personnel sign appropriate access agreements prior to receiving access; |  |
| **PS-6.3.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates the access agreements; and |  |
| **PS-6.4.1** | 1. the organization reviews/updates the access agreements in accordance with the organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **PS-7** | **THIRD-PARTY PERSONNEL SECURITY** | **RESULTS** |
| **PS-7.1** | Determine if: |  |
| **PS-7.1.1** | 1. the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); |  |
| **PS-7.2.1** | 1. the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35; and |  |
| **PS-7.3.1** | 1. the organization monitors third-party provider compliance with personnel security requirements. |  |

|  |  |  |
| --- | --- | --- |
| **PS-8** | **PERSONNEL SANCTIONS** | **RESULTS** |
| **PS-8.1** | Determine if: |  |
| **PS-8.1.1** | 1. the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and |  |
| **PS-8.1.2** | 1. the personnel sanctions process is consistent with applicable laws, Executive Orders, directive, policies, regulations, standards, and guidance. |  |

### Risk Assessment (RA)

|  |  |  |
| --- | --- | --- |
| **RA-1** | **RISK ASSESSMENT POLICY AND PROCEDURES** | **RESULTS** |
| **RA-1.1** | Determine if: |  |
| **RA-1.1.1** | 1. the organization develops and formally documents risk assessment policy; |  |
| **RA-1.1.2** | 1. the organization risk assessment policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **RA-1.1.3** | 1. the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities; |  |
| **RA-1.1.4** | 1. the organization develops and formally documents risk assessment procedures; |  |
| **RA-1.1.5** | 1. the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls; and |  |
| **RA-1.1.6** | 1. the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities. |  |
| **RA-1.2** | Determine if: |  |
| **RA-1.2.1** | 1. the organization defines the frequency of risk assessment policy reviews/updates; |  |
| **RA-1.2.2** | 1. the organization reviews/updates risk assessment policy in accordance with organization-defined frequency; and |  |
| **RA-1.2.3** | 1. the organization defines the frequency of risk assessment procedure reviews/updates; |  |
| **RA-1.2.4** | 1. the organization reviews/updates risk assessment procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **RA-2** | **SECURITY CATEGORIZATION** | **RESULTS** |
| **RA-2.1** | Determine if: |  |
| **RA-2.1.1** | 1. the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials, information system owners, chief information officer, senior agency information security officer, an mission/information owners; |  |
| **RA-2.1.2** | 1. the security categorization is consistent with FIPS 199 and considers the provisional impact levels and special factors in NIST Special Publication 800-60; |  |
| **RA-2.1.3** | 1. the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts; |  |
| **RA-2.1.4** | 1. the organization includes supporting rationale for impact-level decisions as part of the security categorization; and |  |
| **RA-2.1.5** | 1. designated senior-level organizational officials review and approve the security categorizations. |  |

|  |  |  |
| --- | --- | --- |
| **RA-3** | **RISK ASSESSMENT** | **RESULTS** |
| **RA-3.1** | Determine if: |  |
| **RA-3.1.1** | 1. the organization assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and |  |
| **RA-3.1.2** | 1. the risk assessment is consistent with the NIST Special publication 800-30. |  |

|  |  |  |
| --- | --- | --- |
| **RA-5** | **VULNERABILITY SCANNING** | **RESULTS** |
| **RA-5.1** | Determine if: |  |
| **RA-5.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the frequency of vulnerability scans within the information system; |  |
| **RA-5.1.2** | 1. the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency and/or random in accordance with organizational policy and assessment of risk, or when significant new vulnerabilities potentially affecting the system are identified and reported; |  |
| **RA-5.1.3** | 1. the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans; |  |
| **RA-5.1.4** | 1. the organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques; and |  |
| **RA-5.1.5** | 1. the organization freely shares the information obtained from the vulnerability scanning process with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. |  |

|  |  |  |
| --- | --- | --- |
| **RA-5(1)** | **VULNERABILITY SCANNING – CONTROL ENHANCEMENT** | **RESULTS** |
| **RA-5(1).1** | Determine if the organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. |  |

### System and Services Acquisition (SA)

|  |  |  |
| --- | --- | --- |
| **SA-1** | **SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES** | **RESULTS** |
| **SA-1.1** | Determine if: |  |
| **SA-1.1.1** | 1. the organization develops and formally documents system and services acquisition policy; |  |
| **SA-1.1.2** | 1. the organization system and services acquisition policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **SA-1.1.3** | 1. the organization disseminates formal documented system and services acquisition policy to elements within the organization having associated system and services acquisition roles and responsibilities; |  |
| **SA-1.1.4** | 1. the organization develops and formally documents system and services acquisition procedures; |  |
| **SA-1.1.5** | 1. the organization system and services acquisition procedures facilitate implementation of the system and services acquisition policy and associated system and services acquisition controls; and |  |
| **SA-1.1.6** | 1. the organization disseminates formal documented system and services acquisition procedures to elements within the organization having associated system and services acquisition roles and responsibilities. |  |
| **SA-1.2** | Determine if: |  |
| **SA-1.2.1** | 1. the organization defines the frequency of system and services acquisition policy reviews/updates; |  |
| **SA-1.2.2** | 1. the organization reviews/updates system and services acquisition policy in accordance with organization-defined frequency; and |  |
| **SA-1.2.3** | 1. the organization defines the frequency of system and services acquisition procedure reviews/updates; |  |
| **SA-1.2.4** | 1. the organization reviews/updates system and services acquisition procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **SA-2** | **ALLOCATION OF RESOURCES** | **RESULTS** |
| **SA-2.1** | Determine if: |  |
| **SA-2.1.1** | 1. the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system by verifying that the organization:   - defines security requirements for the information system in mission/business   planning;  - establishes a discrete line item for information system security in the   organization’s programming and budgeting documentation; and  - integrates information system security into the capital planning and investment   control process in accordance with the guidance in NIST Special Publication 800-   65. |  |

|  |  |  |
| --- | --- | --- |
| **SA-3** | **LIFE CYCLE SUPPORT** | **RESULTS** |
| **SA-3.1** | Determine if: |  |
| **SA-3.1.1** | 1. the organization manages the information system using a system development life cycle methodology that includes information security considerations; and |  |
| **SA-3.1.2** | 1. the organization uses a system development life cycle that is consistent with NIST Special Publication 800-64. |  |

|  |  |  |
| --- | --- | --- |
| **SA-4** | **ACQUISITIONS** | **RESULTS** |
| **SA-4.1** | Determine if: |  |
| **SA-4.1.1** | 1. the organization includes in acquisition contracts for information systems, either explicitly or by reference, security requirements and/or security specifications based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards that describe required:  * security capabilities; * design and development processes; * test and evaluation procedures; and * documentation. |  |
| **SA-4.2.1** | 1. the organization includes in acquisition contracts, requirements for information system documentation addressing user and systems administrator guidance and information regarding the implementation of the security controls in the system and at a level of detail based on the FIPS 199 security category for the system.; and |  |
| **SA-4.3.1** | 1. the organization includes in acquisition contracts requirements for information system documentation that includes security configuration settings and security implementation guidance. |  |

|  |  |  |
| --- | --- | --- |
| **SA-4(1)** | **ACQUISITIONS – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-4(1).1** | Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. |  |

|  |  |  |
| --- | --- | --- |
| **SA-4(4)** | **ACQUISITIONS – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-4(4).1** | Determine if the organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment. |  |

|  |  |  |
| --- | --- | --- |
| **SA-5** | **INFORMATION SYSTEM DOCUMENTATION** | **RESULTS** |
| **SA-5.1** | Determine if: |  |
| **SA-5.1.1** | 1. the organization obtains, protects as required, and makes available to authorized personnel, information system administrator and user guidance with information on:  * configuring, installing, and operating the information system; and * effectively using the system’s security features; or |  |
| **SA-5.1.2** | 1. the organization, when this information is either unavailable or nonexistent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. |  |

|  |  |  |
| --- | --- | --- |
| **SA-5(1)** | **INFORMATION SYSTEM DOCUMENTATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-5(1).1** | Determine if: |  |
| **SA-5(1).1.1** | 1. the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. |  |

|  |  |  |
| --- | --- | --- |
| **SA-5(3)** | **INFORMATION SYSTEM DOCUMENTATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SA-5(3).1** | Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. |  |

|  |  |  |
| --- | --- | --- |
| **SA-6** | **SOFTWARE USAGE RESTRICTIONS** | **RESULTS** |
| **SA-6.1** | Determine if: |  |
| **SA-6.1.1** | 1. the organization complies with software usage restrictions; and |  |
| **SA-6.1.2** | 1. the organization employs tracking systems to control copying and distribution of software and associated documentation protected by quantity licenses; and |  |
| **SA-6.1.3** | 1. the organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. |  |

|  |  |  |
| --- | --- | --- |
| **SA-7** | **USER INSTALLED SOFTWARE** | **RESULTS** |
| **SA-7.1** | Determine if the organization enforces explicit rules governing the installation of software by users that include organization-identified types of software installations that are permitted and types of installations that are prohibited. |  |

|  |  |  |
| --- | --- | --- |
| **SA-8** | **SECURITY ENGINEERING PRINCIPLES** | **RESULTS** |
| **SA-8.1** | Determine if: |  |
| **SA-8.1.1** | 1. the organization designs and implements the information system using security engineering principles; and |  |
| **SA-8.1.2** | 1. the organization considers the security design principles in NIST Special Publication 800-27 in the design, development, and implementation of the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SA-9** | **EXTERNAL INFORMATION SYSTEM SERVICES** | **RESULTS** |
| **SA-9.1** | Determine if: |  |
| **SA-9.1.1** | 1. the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directive, policies, regulations, standards, guidance, and established service-level agreements; and |  |
| **SA-9.1.2** | 1. the organization monitors security control compliance. |  |

|  |  |  |
| --- | --- | --- |
| **SA-10** | **DEVELOPER CONFIGURATION MANAGEMENT** | **RESULTS** |
| **SA-10.1** | Determine if the organization requires that information system developers/integrators: |  |
| **SA-10.1.1** | 1. Perform configuration management during information system design, development, implementation, and operation; |  |
| **SA-10.1.2** | 1. Manage and control changes to the information system; |  |
| **SA-10.1.3** | 1. Implement only organization-approved changes; |  |
| **SA-10.1.4** | 1. Document approved changes to the information system; and |  |
| **SA-10.1.5** | 1. Track security flaws and flaw resolution. |  |

|  |  |  |
| --- | --- | --- |
| **SA-11** | **DEVELOPER SECURITY TESTING** | **RESULTS** |
| **SA-11.1** | Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results. |  |

### System and Communication Protection (SC)

|  |  |  |
| --- | --- | --- |
| **SC-1** | **SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES** | **RESULTS** |
| **SC-1.1** | Determine if: |  |
| **SC-1.1.1** | 1. the organization develops and formally documents system and communications protection policy; |  |
| **SC-1.1.2** | 1. the organization system and communications protection policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **SC-1.1.3** | 1. the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities; |  |
| **SC-1.1.4** | 1. the organization develops and formally documents system and communications protection procedures; |  |
| **SC-1.1.5** | 1. the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls; and |  |
| **SC-1.1.6** | 1. the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities. |  |
| **SC-1.2** | Determine if: |  |
| **SC-1.2.1** | 1. the organization defines the frequency of system and communications protection policy reviews/updates; |  |
| **SC-1.2.2** | 1. the organization reviews/updates system and communications protection policy in accordance with organization-defined frequency; and |  |
| **SC-1.2.3** | 1. the organization defines the frequency of system and communications protection procedure reviews/updates; |  |
| **SC-1.2.4** | 1. the organization reviews/updates system and communications protection procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **SC-2** | **APPLICATION PARTITIONING** | **RESULTS** |
| **SC-2.1** | Determine if: |  |
| **SC-2.1.1** | 1. the information system separates user functionality (including user interface services) from information system management functionality. |  |

|  |  |  |
| --- | --- | --- |
| **SC-4** | **INFORMATION IN SHARED RESOURCES** | **RESULTS** |
| **SC-4.1** | Determine if the information system prevents unauthorized and unintended information transfer via shared system resources. |  |

|  |  |  |
| --- | --- | --- |
| **SC-5** | **DENIAL OF SERVICE PROTECTION** | **RESULTS** |
| **SC-5.1** | Determine if: |  |
| **SC-5.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and |  |
| **SC-5.1.2** | 1. the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7** | **BOUNDARY PROTECTION** | **RESULTS** |
| **SC-7.1** | Determine if: |  |
| **SC-7.1.1** | 1. the organization defines key internal boundaries of the information system; and |  |
| **SC-7.2.1** | 1. the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(1)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(1).1** | Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(2)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(2).1** | Determine if: |  |
| **SC-7(2).1.1** | 1. the organization defines the mediation necessary for public access to the organization’s internal networks; and |  |
| **SC-7(2).2.1** | 1. the organization prevents public access into the organization’s internal networks except as appropriately mediated. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(3)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(3).1** | Determine if the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(4)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(4).1** | Determine if the organization implements a managed interface (boundary protection devices in effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(5)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(5).1** | Determine if the information system denies network traffic by default and allows network traffic by exception. |  |

|  |  |  |
| --- | --- | --- |
| **SC-7(7)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-7(7).1** | Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. |  |

|  |  |  |
| --- | --- | --- |
| **SC-8** | **TRANSMISSION INTEGRITY** | **RESULTS** |
| **SC-8.1** | Determine if the information system protects the integrity of transmitted information. |  |

|  |  |  |
| --- | --- | --- |
| **SC-8(1)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-8(1).1** | Determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. |  |

|  |  |  |
| --- | --- | --- |
| **SC-9** | **TRANSMISSION CONFIDENTIALITY** | **RESULTS** |
| **SC-9.1** | Determine if the information system protects the confidentiality of transmitted information. |  |

|  |  |  |
| --- | --- | --- |
| **SC-9(1)** | **BOUNDARY PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SC-9(1).1** | Determine if organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. |  |

|  |  |  |
| --- | --- | --- |
| **SC-10** | **NETWORK DISCONNECT** | **RESULTS** |
| **SC-10.1** | Determine if: |  |
| **SC-10.1.1** | 1. the organization defines in the security plan, explicitly or by reference, the time period of inactivity before the information system terminates a network connection; and |  |
| **SC-10.2.1** | 1. the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity. |  |

|  |  |  |
| --- | --- | --- |
| **SC-12** | **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT** | **RESULTS** |
| **SC-12.1** | Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-13** | **USE OF CRYPTOGRAPHY** | **RESULTS** |
| **SC-13.1** | Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. |  |

|  |  |  |
| --- | --- | --- |
| **SC-14** | **PUBLIC ACCESS PROTECTIONS** | **RESULTS** |
| **SC-14.1** | Determine if the information system protects the integrity and availability of publicly available information and applications. |  |

|  |  |  |
| --- | --- | --- |
| **SC-15** | **COLLABORATIVE COMPUTING** | **RESULTS** |
| **SC-15.1** | Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. |  |

|  |  |  |
| --- | --- | --- |
| **SC-17** | **PUBLIC KEY INFRASTRUCTURE CERTIFICATES** | **RESULTS** |
| **SC-17.1** | Determine if the organization issues public key certificates under an appropriate certificates policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. |  |

|  |  |  |
| --- | --- | --- |
| **SC-18** | **MOBILE CODE** | **RESULTS** |
| **SC-18.1** | Determine if: |  |
| **SC-18.1.1** | 1. the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and |  |
| **SC-18.2.1** | 1. the organization authorizes, monitors, and controls the use of mobile code within the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-19** | **VOICE OVER INTERNET PROTOCOL** | **RESULTS** |
| **SC-19.1** | Determine if: |  |
| **SC-19.1.1** | 1. the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and |  |
| **SC-19.2.1** | 1. the organization authorizes, monitors, and controls the use of VoIP within the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SC-20** | **SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)** | **RESULTS** |
| **SC-20.1** | Determine if the information system, (if the system provides a name/address resolution service), provides artifacts for additional data origin with authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries. |  |

|  |  |  |
| --- | --- | --- |
| **SC-22** | **ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE** | **RESULTS** |
| **SC-22.1** | Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation. |  |

|  |  |  |
| --- | --- | --- |
| **SC-23** | **SESSION AUTHENTICITY** | **RESULTS** |
| **SC-23.1** | Determine if the information system provides mechanisms to protect the authenticity of communications sessions. |  |

|  |  |  |
| --- | --- | --- |
| **SC-28** | **PROTECTION OF INFORMATION AT REST** | **RESULTS** |
| **SC-28.1** | Determine if the information system protects the confidentiality and integrity of information at rest. |  |

|  |  |  |
| --- | --- | --- |
| **SC-32** | **INFORMATION SYSTEM PARTITIONING** | **RESULTS** |
| **SC-32.1** | Determine if the organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. |  |

### System and Information Integrity (SI)

|  |  |  |
| --- | --- | --- |
| **SI-1** | **SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES** | **RESULTS** |
| **SI-1.1** | Determine if: |  |
| **SI-1.1.1** | 1. the organization develops and formally documents system and information integrity policy; |  |
| **SI-1.1.2** | 1. the organization system and information integrity policy addresses:  * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance; |  |
| **SI-1.1.3** | 1. the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities; |  |
| **SI-1.1.4** | 1. the organization develops and formally documents system and information integrity procedures; |  |
| **SI-1.1.5** | 1. the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls; and |  |
| **SI-1.1.6** | 1. the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities. |  |
| **SI-1.2** | Determine if: |  |
| **SI-1.2.1** | 1. the organization defines the frequency of system and information integrity policy reviews/updates; |  |
| **SI-1.2.2** | 1. the organization reviews/updates system and information integrity policy in accordance with organization-defined frequency; and |  |
| **SI-1.2.3** | 1. the organization defines the frequency of system and information integrity procedure reviews/updates; |  |
| **SI-1.2.4** | 1. the organization reviews/updates system and information integrity procedures in accordance with organization-defined frequency. |  |

|  |  |  |
| --- | --- | --- |
| **SI-2** | **FLAW REMEDIATION** | **RESULTS** |
| **SI-2.1** | Determine if: |  |
| **SI-2.1.1** | 1. the organization identifies, reports, and corrects information system flaws; |  |
| **SI-2.1.2** | 1. the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures; |  |
| **SI-2.1.3** | 1. the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures; |  |
| **SI-2.1.4** | 1. the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and |  |
| **SI-2.1.5** | 1. the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned. |  |

|  |  |  |
| --- | --- | --- |
| **SI-2(2)** | **FLAW REMEDIATION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-2(2).1** | Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3** | **MALICIOUS CODE PROTECTION** | **RESULTS** |
| **SI-3.1** | Determine if the information system implements malicious code protection by verifying that:   * the organization employs malicious code protection mechanisms at critical information system entry and exit points, and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code; * the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities; * the organization updates malicious code protection mechanisms whenever new releases are available, to include the latest malicious code definitions, in accordance with organizational configuration management policy and procedures; * the organization considered use of malicious code protection software products from multiple vendors; and * the organization considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3(1)** | **MALICIOUS CODE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-3(1).1** | Determine if the organization centrally manages malicious code protection mechanisms. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3(2)** | **MALICIOUS CODE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-3(2).1** | Determine if the organization automatically updates malicious code protection mechanisms. |  |

|  |  |  |
| --- | --- | --- |
| **SI-3(3)** | **MALICIOUS CODE PROTECTION – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-3(3).1** | Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4** | **INFORMATION SYSTEM MONITORING** | **RESULTS** |
| **SI-4.1** | Determine if: |  |
| **SI-4.1.1** | 1. the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system; |  |
| **SI-4.1.2** | 1. the organization deploys monitoring devices strategically within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information; |  |
| **SI-4.1.3** | 1. the organization deploys monitoring devices at ad hoc locations within the information system to track specific transactions; |  |
| **SI-4.1.4** | 1. the organization uses the monitoring devices to track the impact of security changes to the information system; |  |
| **SI-4.1.5** | 1. the organization determines the granularity of the information collected based upon it’s monitoring objectives and the capability of the information system to support such activities; |  |
| **SI-4.1.6** | 1. the organization consults appropriate legal counsel with regard to all information system monitoring activities; and |  |
| **SI-4.1.7** | 1. the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation, based on law enforcement information, intelligence information, or other credible sources of information. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(2)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(2).1** | Determine if the organization employs automated tools to support near real-time analysis of events. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(4)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(4).1** | Determine if information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(5)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(5).1** | Determine if the information system provides near real-time alerts when the following indications of compromise or potential compromise occur:[See audit logging process documentation] |  |

|  |  |  |
| --- | --- | --- |
| **SI-4(6)** | **INFORMATION SYSTEM MONITORING – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-4(6).1** | Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities. |  |

|  |  |  |
| --- | --- | --- |
| **SI-5** | **SECURITY ALERTS AND ADVISORIES** | **RESULTS** |
| **SI-5.1** | Determine if: |  |
| **SI-5.1.1** | 1. the organization receives information system security alerts/advisories on a regular basis; |  |
| **SI-5.2.1** | 1. the organization issues security alerts/advisories to appropriate organizational personnel; |  |
| **SI-5.3.1** | 1. the organization takes appropriate actions in response to security alerts/advisories; and |  |
| **SI-5.4.1** | 1. the organization maintains contact with special interest groups (e.g., information security forums) that:  * facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); * provide access to advice from security professionals; and * improve knowledge of security best practices. |  |

|  |  |  |
| --- | --- | --- |
| **SI-7** | **SOFTWARE AND INFORMATION INTEGRITY** | **RESULTS** |
| **SI-7.1** | Determine if the information system detects unauthorized changes to software and information. |  |

|  |  |  |
| --- | --- | --- |
| **SI-7(1)** | **SOFTWARE AND INFORMATION INTEGRITY – CONTROL ENHANCEMENT** | **RESULTS** |
| **SI-7(1).1** | Determine if the organization reassesses the integrity of software and information by performing weekly checks. |  |

|  |  |  |
| --- | --- | --- |
| **SI-8** | **SPAM PROTECTION** | **RESULTS** |
| **SI-8.1** | Determine if the information system implements spam protection by verifying that the organization:   * employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network; and * employs spam protection mechanisms to detect and take appropriate action on unsolicited message transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. |  |

|  |  |  |
| --- | --- | --- |
| **SI-9** | **INFORMATION INPUT RESTRICTIONS** | **RESULTS** |
| **SI-9.1** | Determine if the organization restricts the capability to input information to the information system to authorized personnel. |  |

|  |  |  |
| --- | --- | --- |
| **SI-10** | **INFORMATION INPUT VALIDATION** | **RESULTS** |
| **SI-10.1** | Determine if the information system checks information for accuracy, completeness, validity, and authenticity by verifying that the system:   * checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible; * employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content; * prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands; and * checks the accuracy, completeness, validity, and authenticity of information to the extent guided by organizational policy and operational requirements. |  |

|  |  |  |
| --- | --- | --- |
| **SI-11** | **ERROR HANDLING** | **RESULTS** |
| **SI-11.1** | Determine if: |  |
| **SI-11.1.1** | 1. the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries; |  |
| **SI-11.2.1** | 1. the information system reveals error messages only to authorized individuals; and |  |
| **SI-11.3.1** | 1. the information system does not include sensitive information in error logs or associated administrative messages. |  |

|  |  |  |
| --- | --- | --- |
| **SI-12** | **INFORMATION OUTPUT HANDLING AND RETENTION** | **RESULTS** |
| **SI-12.1** | Determine if: |  |
| **SI-12.1.1** | 1. the organization handles output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and |  |
| **SI-12.2.1** | 1. the organization retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. |  |

### Information Security Program Management (PM)

|  |  |  |
| --- | --- | --- |
| **PM-1** | **INFORMATION SECURITY PROGRAM PLAN** | **RESULTS** |
| **PM-1.1** | Determine if: |  |
| **PM-1.1.1** | 1. the organization develops an information security program plan for the organization   that:   * provides an overview of the requirements for the security program; * provides a description of the security program management controls and   common controls in place or planned for meeting security program  requirements;   * provides sufficient information about the program management controls and   common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;   * includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; * is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation; |  |
| **PM-1.1.2** | 1. Reviews the organization-wide information security program plan ***annually***; and |  |
| **PM-1.1.3** | 1. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments. |  |

|  |  |  |
| --- | --- | --- |
| **PM-2** | **SENIOR INFORMATION SECURITY OFFICER** | **RESULTS** |
| **PM-2.1** | Determine if: |  |
| **PM-2.1.1** | 1. organization appoints a senior information security officer to coordinate, develop, implement, and maintain an organization-wide information security program; and |  |
| **PM-2.1.2** | 1. the organization empowers the senior information security officer with the mission and resources required to coordinate, develop, implement, and maintain an organization-wide information security program. |  |

|  |  |  |
| --- | --- | --- |
| **PM-3** | **INFORMATION SECURITY RESOURCES** | **RESULTS** |
| **PM-3.1** | Determine if: |  |
| **PM-3.1.1** | 1. the organization includes in its capital planning and investment requests the resources needed to implement the information security program; |  |
| **PM-3.1.2** | 1. the organization documents all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program; |  |
| **PM-3.1.3** | 1. the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and |  |
| **PM-3.1.4** | 1. the organization makes the required information security resources available for expenditure as planned. |  |

|  |  |  |
| --- | --- | --- |
| **PM-4** | **PLAN OF ACTION AND MILESTONES PROCESS** | **RESULTS** |
| **PM-4.1** | Determine if: |  |
| **PM-4.1.1** | 1. the organization implements a process to maintain plans of action and milestones for the security program and the associated organizational information systems; and |  |
| **PM-4.1.2** | 1. the organization implements a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. |  |

|  |  |  |
| --- | --- | --- |
| **PM-5** | **INFORMATION SYSTEM INVENTORY** | **RESULTS** |
| **PM-5.1** | Determine if: |  |
| **PM-5.1.1** | 1. the organization develops an inventory of its information systems; and |  |
| **PM-5.1.2** | 1. the organization maintains an inventory of its information systems. |  |

|  |  |  |
| --- | --- | --- |
| **PM-6** | **INFORMATION SECURITY MEASURES OF PERFORMANCE** | **RESULTS** |
| **PM-6.1** | Determine if: |  |
| **PM-6.1.1** | 1. the organization develops information security measures of performance; |  |
| **PM-6.1.2** | 1. the organization monitors information security measures of performance; and |  |
| **PM-6.1.3** | 1. the organization reports on the results of information security measures of performance. |  |

|  |  |  |
| --- | --- | --- |
| **PM-7** | **ENTERPRISE ARCHITECTURE** | **RESULTS** |
| **PM-7.1** | Determine if the organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. |  |

|  |  |  |
| --- | --- | --- |
| **PM-8** | **CRITICAL INFRASTRUCTURE PLAN** | **RESULTS** |
| **PM-8.1** | Determine if: |  |
| **PM-8.1.1** | 1. the organization develops and documents a critical infrastructure and key resource protection plan; |  |
| **PM-8.1.2** | 1. the organization updates the critical infrastructure and key resource protection plan; and |  |
| **PM-8.1.3** | 1. the organization addresses information security issues in the critical infrastructure and key resource protection plan. |  |

|  |  |  |
| --- | --- | --- |
| **PM-9** | **RISK MANAGEMENT STRATEGY** | **RESULTS** |
| **PM-9.1** | Determine if: |  |
| **PM-9.1.1** | 1. the organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and |  |
| **PM-9.1.2** | 1. the organization implements that strategy consistently across the organization. |  |

|  |  |  |
| --- | --- | --- |
| **PM-10** | **SECURITY AUTHORIZATION PROCESS** | **RESULTS** |
| **PM-10.1** | Determine if: |  |
| **PM-10.1.1** | 1. the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; |  |
| **PM-10.1.2** | 1. the organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and |  |
| **PM-10.1.3** | 1. the organization fully integrates the security authorization processes into an organization-wide risk management program. |  |

|  |  |  |
| --- | --- | --- |
| **PM-11** | **MISSION / BUSINESS PROCESS DEFINITION** | **RESULTS** |
| **PM-11.1** | Determine if: |  |
| **PM-11.1.1** | 1. the organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and |  |
| **PM-11.1.2** | 1. the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. |  |

## GLBA Safeguards Rule

### General Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Requirement | Control Effectiveness | Notes |
| G1 | Develop a written information security plan. |  |  |
| G2 | Designate one or more employees to coordinate the information security program. |  |  |
| G3 | Identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks. |  |  |
| G4 | Design and implement a safeguards program, and regularly monitor and test it. |  |  |
| G5 | Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information. |  |  |
| G6 | Evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business or operations, or the results of security testing and monitoring. |  |  |

### Employee Management and Training

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Requirement | Control Effectiveness | Notes |
| E1 | Check references or do background checks before hiring employees who will have access to customer information. |  |  |
| E2 | Require every new employee to sign an agreement to follow your company’s confidentiality and security standards for handling customer information. |  |  |
| E3 | Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs. |  |  |
| E4 | Control access to sensitive information by requiring employees to use “strong” passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) |  |  |
| E5 | Use password-activated screen savers to lock employee computers after a period of inactivity. |  |  |
| E6 | Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device. |  |  |
| E7 | Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. |  |  |
| E8 | Regularly remind all employees of your company’s policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms. |  |  |
| E9 | Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions. |  |  |
| E10 | Impose disciplinary measures for security policy violations. |  |  |
| E11 | Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures. |  |  |

### Information Systems

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Requirement | Control Effectiveness | Notes |
| I1 | Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods. |  |  |
| I2 | Store records in a room or cabinet that is locked when unattended. |  |  |
| I3 | When customer information is stored on a server or other computer, ensure that the computer is accessible only with a “strong” password and is kept in a physically-secure area. |  |  |
| I4 | Where possible, avoid storing sensitive customer data on a computer with an Internet connection. |  |  |
| I5 | Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area. |  |  |
| I6 | Maintain a careful inventory of your company’s computers and any other equipment on which customer information may be stored. |  |  |
| I7 | When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. |  |  |
| I8 | If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message. |  |  |
| I9 | If you must transmit sensitive data by email over the Internet, be sure to encrypt the data. |  |  |
| I10 | Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group. |  |  |
| I11 | Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed. |  |  |
| I12 | Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information. |  |  |

### Detecting and Managing System Failures

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Requirement | Control Effectiveness | Notes |
| D1 | Monitor the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses. |  |  |
| D2 | Check with software vendors regularly to get and install patches that resolve software vulnerabilities. |  |  |
| D3 | Use anti-virus and anti-spyware software that updates automatically. |  |  |
| D4 | Maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations. |  |  |
| D5 | Regularly ensure that ports not used for your business are closed. |  |  |
| D6 | Promptly pass along information and instructions to employees regarding any new security risks or possible breaches. |  |  |
| D7 | Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information. |  |  |
| D8 | Use an up-to-date intrusion detection system to alert you of attacks. |  |  |
| D9 | Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. |  |  |
| D10 | Take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet. |  |  |
| D11 | Preserve and review files or programs that may reveal how a breach occurred. |  |  |
| D12 | If feasible and appropriate, bring in security professionals to help assess a breach as soon as possible. |  |  |
| D13 | Notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm. |  |  |
| D14 | Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm |  |  |
| D15 | Notify the credit bureaus and other businesses that may be affected by the breach. |  |  |
| D16 | Check to see if breach notification is required under applicable state law. |  |  |

## GLBA Safeguards Rule

### General Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **G1** Develop a written information security plan. | | | |
| **G1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **G2** Designate one or more employees to coordinate the information security program. | | | |
| **G2** Examine information security policies and procedures to verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. | **Identify** **the information security policies** reviewed to verify the specific and formal assignment of the information security to a Chief Security Officer or other security-knowledgeable member of management. |  |  |
| **G3** Identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks. | | | |
| **G3.a** Verify that an annual risk-assessment process is documented that:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. | **Describe how** it was verified that an annual risk-assessment process is documented that: | |  |
| * Identifies critical assets, threats and vulnerabilities. |  |
| * Results in formal, documented analysis of risk. |  |
| **G3.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | **Identify the risk assessment result documentation** reviewed to verify that:   * The risk assessment process is performed at least annually. * The risk assessment is performed upon significant changes to the environment. * The documented risk assessment process was followed. |  |  |
| **G4** Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information. | | | |
| **G4.a** Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom customer information is shared, or that could affect the security of customer information (for example, backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.), as follows: | **Identify the documented policies and procedures to manage service providers with whom customer information is shared, or that could affect the security of customer information**, reviewed to verify policy defines the following:   * Maintain a list of service providers. * Maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable GLBA requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s information, or manages the customer's network, applications or systems on behalf of a customer. * Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. |  |  |
| **G4.b** Verify that a list of service providers is maintained. | **Describe how** the documented list of service providers was observed to be maintained (kept up-to-date). |  |  |
| **G4.c** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of customer data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s network, applications or systems. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable GLBA requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer data, or manages the customer's network, applications or systems on behalf of a customer. |  |  |
| **G4.d** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Describe how** it was verified that the procedures for proper due diligence prior to engaging a service provider are implemented. |  |  |

### Employee Management and Training

|  |  |  |  |
| --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **E1** Check references or do background checks before hiring employees who will have access to customer information. | | | |
| **E1** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to customer data or the customer data environment. | **Identify the documented policy** reviewed to verify requirement for background checks to be conducted:   * On potential personnel who will have access to customer data or the customer data environment. * Prior to hiring the personnel. |  |  |
| **Identify the Human Resources personnel** interviewed who confirm background checks are conducted:   * On potential personnel who will have access to customer data or the customer data environment. * Prior to hiring the personnel. |  |
| **Describe how** it was verified that background checks are conducted (within the constraints of local laws): | |
| * On potential personnel who will have access to customer data or the customer data environment. |  |
| * Prior to hiring the personnel. |  |
| **E2** Require every new employee to sign an agreement to follow your company’s confidentiality and security standards for handling customer information. | | | |
| **E2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. | **Describe how** it was verified that, per the security awareness program, all personnel: | |  |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  |
| * Provide an acknowledgement at least annually. |  |
| **E3** Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs. | | | |
| **E3** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | * **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **E4** Control access to sensitive information by requiring employees to use “strong” passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) | | | |
| **E4** For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | **Identify the sample** of system components selected for this testing procedure. |  |  |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that user password parameters are set to require at least the following strength/complexity: | |
| * Require a minimum length of at least seven characters. |  |
| * Contain both numeric and alphabetic characters. |  |
| **E5** Use password-activated screen savers to lock employee computers after a period of inactivity. | | | |
| **E5** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** **the sample** of system components selected for this testing procedure. |  |  |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that system/session idle time out features have been set to 15 minutes or less. |  |
| **E6** Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device. | | | |
| **E6** Verify that the usage policies define acceptable uses for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  |  |
| **E7** Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. | | | |
| **E7** Review the security awareness training documentation to verify it provides awareness to all personnel about the importance of protecting customer information. | **Identify** the documented security awareness training documentation reviewed to verify it includes at least the following topics:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. |  |  |
| **E8** Regularly remind all employees of your company’s policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms. | | | |
| **E8** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe** how the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **E9** Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions. | | | |
| **E9** Verify that telecommuting policies specify in detail at a minimum, the following:   * Whether or how employees are allowed to keep or access customer data at home * Requirement for employees who use personal computers or access cuistomer data to use adequate protection measures (anti-virus, firewall, patching, etc.) | **Identify** the documented telecommuting policy reviewed to verify it includes at least the following topics:   * Whether or how employees are allowed to keep or access customer data at home * Requirement for employees who use personal computers or access cuistomer data to use adequate protection measures (anti-virus, firewall, patching, etc.) |  |  |
| **E10** Impose disciplinary measures for security policy violations. | | | |
| **E10** Inquire with Human Resource department management and verify that employees are sanctioned when they violate security policies. | **Identify** the Human Resources personnel interviewed who confirm that employees are sanctioned when they violate security policies. |  |  |
| **E11** Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures. | | | |
| **E11.a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** the sample of users terminated in the past six months selected. |  |  |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **E11.b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  |  |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  |

### Information Systems

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** | |
| **I1** Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods. | | | | |
| **I1** Verify the existence of environmental security controls for each computer room, data center, and other storage areas containing customer data. | **Identify and briefly describe** all of the storage areas containing customer data: | |  | |
| All computer rooms |  |
| All data centers |  |
| Any other physical areas |  |
| *For each identified area, complete the following*: | |
| Describe the environmental security controls to be in place |  |
| **I2** Store records in a room or cabinet that is locked when unattended. | | | | |
| **I2** Observe the storage location’s physical security to confirm that all records storage is secure. | **Identify** all locations where customer records are stored. |  |  | |
| **Describe how** it was observed that customer records are stored in a secure location. |  |
| **I3** When customer information is stored on a server or other computer, ensure that the computer is accessible only with a “strong” password and is kept in a physically-secure area. | | | | |
| **I3** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the customer data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. * Observe a system administrator’s attempt to log into consoles for randomly selected systems in the customer data environment and verify that they are “locked” to prevent unauthorized use. | **Identify and briefly describe** all of the storage areas containing customer data: | |  | |
| All computer rooms |  |
| All data centers |  |
| Any other physical areas |  |
| *For each identified area, complete the following*: |  |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **Identify** the randomly selected systems in the cardholder environment for which a system administrator login attempt was observed. |  |
| **Describe how** consoles for the randomly selected systems were observed to verify that they are “locked” when not in use to prevent unauthorized use. |  |
| **I4** Where possible, avoid storing sensitive customer data on a computer with an Internet connection. | | | | |
| **I4** Verify that all systems that store sensitive customer data either do not have an Internet connection, or must (for business or technical reasons) have an Internet connection. | **Identify and briefly describe** all computers that store sensitive customer data and have an Internet connection. |  | |  |
| *For each computer that stores sensitive consumer data and has an Internet connection,* complete the following: | | |
| **Describe** the reason why the computer must have an Internet connection. |  | |
| **I5** Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area. | | | | |
| **I5.a** Observe the storage location’s physical security to confirm that backup media storage is secure. | **Identify** all locations where backup media is stored. |  |  | |
| **Describe how** it was observed that backup media storage is stored in a secure location. |  |
| **I5.b** Verify that the storage location security is reviewed at least annually. | **Identify** the document reviewed to verify that the storage location must be reviewed at least annually. |  |  | |
| **Describe how** processes were observed to verify that reviews of the security of each storage location are performed at least annually. |  |
| **I6** Maintain a careful inventory of your company’s computers and any other equipment on which customer information may be stored. | | | | |
| **I6.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. | **Describe how** the system inventory was examined to verify that a list of hardware and software components is: | |  | |
| * Maintained |  |
| * Includes a description of function/use for each |  |
| **I6.b** Interview personnel to verify the documented inventory is kept current. | **Identify** the personnel interviewed for this testing procedure. |  |  | |
| For the interview, **summarize the relevant details** discussed that verify that the documented inventory is kept current. |  |
| **I7** When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. | | | | |
| **I7.a** Identify all locations where cardholder data or other sensitive financial data is transmitted or received over open, public networks. Examine system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where cardholder data or other sensitive financial data is transmitted or received over open, public networks. |  |  | |
| **I7.b** Select and observe a sample of inbound and outbound transmissions as they occur to verify that all cardholder data or other sensitive financial data is encrypted with strong cryptography during transit. | **Describe** the sample of inbound and outbound transmissions observed as they occurred. |  |  | |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all cardholder data is encrypted with strong cryptography during transit. |  |
| **I8** If you collect information online directly from customers, make secure transmission automatic. | | | | |
| **I8** Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. | *For all instances where customer data Is transmitted or received over open, public networks,* **describe how** system configurations were observed to verify that the protocol is implemented: | |  | |
| To use only secure configurations. |  |
| Does not support insecure versions or configurations. |  |
| **I9** If you must transmit sensitive data by email over the Internet, be sure to encrypt the data. | | | | |
| **I9.a** If end-user messaging technologies are used to send sensitive data, observe processes for sending sensitive data and examine a sample of outbound transmissions as they occur to verify that sensitive data is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | **Identify** whether end-user messaging technologies are used to send cardholder data. **(yes/no)** |  |  | |
| *If “no,” mark the remainder of I9.a as “Not Applicable” and proceed to I9.b.*  *If “yes,” complete the following:* | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **Describe** the sample of outbound transmissions observed as they occurred to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **I9.b** Review written policies to verify the existence of a policy stating that unprotected sensitive data are not to be sent via end-user messaging technologies. | *If “no” at I9.a:* | |  | |
| **Identify** the policy document that explicitly prohibits sensitive data from being sent via end-user messaging technologies under any circumstance. |  |
| *If “yes” at I9.a:* | |
| **Identify** the policy document stating that unprotected sensitive data must not be sent via end-user messaging technologies. |  |
| **I10** Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group. | | | | |
| **I10.a** Verify that responsibility for records retention and disposal has been formally assigned. | Provide the name of the assessor who attests that responsibility for records retention and disposal has been formally assigned. |  |  | |
| **I10.b** If an outside disposal company is used, verify that the company has been certified by a recognized industry group. | Provide the name of the assessor who attests that the company has been certified by a recognized industry group. |  |  | |
| **I11** Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed. | | | | |
| **I11** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | **Identify** personnel interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  |  | |
| **Describe how** the procedures were examined to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. |  |
| **I12** Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information. | | | | |
| **I12** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media. | **Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. |  |  | |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify** the industry-accepted standards used. |  |

### Detecting and Managing System Failures

|  |  |  |  |
| --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **D1** Monitor the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses. | | | |
| **D1** Interview responsible personnel and observe processes to verify that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. | * **Identify** the responsible personnel interviewed who confirm that: * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  |  |
| **Describe** the processes observed to verify that: | |
| New security vulnerabilities are identified. |  |
| A risk ranking is assigned to vulnerabilities to include identification of all “high” risk and “critical” vulnerabilities. |  |
| Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  |
| Identify the outside sources used. |  |
| **D2** Check with software vendors regularly to get and install patches that resolve software vulnerabilities. | | | |
| **D2** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:   * That applicable critical vendor-supplied security patches are installed within one month of release. * All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). | **Identify** **the sample** of system components and related software selected for this testing procedure. |  |  |
| **Identify** the vendor security patch list reviewed. |  |
| *For each item in the sample,* **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify that: | |
| Applicable critical vendor-supplied security patches are installed within one month of release. |  |
| All applicable vendor-supplied security patches are installed within an appropriate time frame. |  |
| **D3** Use anti-virus and anti-spyware software that updates automatically. | | | |
| **D3.a** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components selected (including all operating system types commonly affected by malicious software). |  |  |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  |
| **D3.b** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | * **Identify** the vendor documentation reviewed to verify that anti-virus programs: * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| Detect all known types of malicious software, |  |
| Remove all known types of malicious software, and |  |
| Protect against all known types of malicious software. |  |
| **D3.c** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are configured to perform automatic updates. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are Configured to perform automatic updates. |  |  |
| **D4** Maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations. | | | |
| **D4** Examine firewall configurations to verify they are up-to-date. | **Describe how** firewall configurations were examined to verify the firewalls are up-to-date. |  |  |
| **D5** Regularly ensure that ports not used for your business are closed. | | | |
| **D5.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. | **Identify** the firewall and router configuration standards reviewed to verify they require a review of firewall rule sets at least every six months. |  |  |
| **D5.b** Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. | **Identify** the document(s) relating to rule set reviews that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets. |  |  |
| **Identify the responsible personnel interviewed** who confirm that rule sets are reviewed at least every six months for firewall and router rule sets. |  |
| **D6** Promptly pass along information and instructions to employees regarding any new security risks or possible breaches. | | | |
| **D6** Verify that that information and instructions are promptly passed along to employees regarding any new security risks or possible breaches. | Provide the name of the assessor who attests that information and instructions are promptly passed along to employees regarding any new security risks or possible breaches. |  |  |
| **D7** Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information. | | | |
| **D7.a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | * **Identify** the documented security policies and procedures examined to verify that procedures define reviewing the following at least daily, either manually or via log tools: * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components. * Logs of all servers and system components that perform security functions. |  |  |
| Describe the manual or log tools used for daily review of logs. |  |
| **D7.b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | * **Identify** the personnel interviewed who confirm that the following are reviewed at least daily: * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | |
| All security events. |  |
| Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. |  |
| Logs of all critical system components. |  |
| Logs of all servers and system components that perform security functions. |  |
| **D8** Use an up-to-date intrusion detection system to alert you of attacks. | | | |
| **D8** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | **Identify** the vendor document(s) examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques |  |  |
| **Describe how** IDS/IPS configurations were examined and compared to vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are: | |
| Configured per vendor instructions to ensure optimal protection. |  |
| Maintained per vendor instructions to ensure optimal protection. |  |
| Updated per vendor instructions to ensure optimal protection. |  |
| **D9** Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. | | | |
| **D9** Verify that in- and out-bound transfers of infortmation are monitored for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. | **Descibe how** processes were observed to Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. |  |  |
| **D10** Take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet. | | | |
| **D10** Verify that the incident response plan includes specific incident response procedures. | Provide the name of the assessor who attests that the incident response plan includes specific incident response procedures. |  |  |
| **D11** Preserve and review files or programs that may reveal how a breach occurred. | | | |
| **D11** Verify that the incident response plan includes evidence gathering and retention requirements. | Provide the name of the assessor who attests that the incident response plan includes evidence gathering and retention requirements. |  |  |
| **D12** If feasible and appropriate, bring in security professionals to help assess a breach as soon as possible. | | | |
| **D12** Verify that the incident response plan includes contact information for security professionals if feasible and appropriate to help assess a breach as soon as possible. | Provide the name of the assessor who attests that the incident response plan includes contact information for security professionals if feasible and appropriate to help assess a breach as soon as possible |  |  |
| **D13** Notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm. | | | |
| **D13** Verify that the incident response plan includes procedures for notifying consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm. | Provide the name of the assessor who attests that the incident response plan includes procedures for notifying consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm. |  |  |
| **D14** Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm. | | | |
| **D14** Verify that the incident response plan includes procedures for notifying law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm. | Provide the name of the assessor who attests that the incident response plan includes procedures for notifying law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm. |  |  |
| **D15** Notify the credit bureaus and other businesses that may be affected by the breach. | | | |
| **D15** Verify that the incident response plan includes procedures for notifying the credit bureaus and other businesses that may be affected by the breach. | Provide the name of the assessor who attests that the incident response plan includes procedures for notifying the credit bureaus and other businesses that may be affected by the breach. |  |  |
| **D16** Check to see if breach notification is required under applicable state law. | | | |
| **D16** Verify that the incident response plan includes analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). | Provide the name of the assessor who attests that the incident response plan includes analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). |  |  |

## GLBA Safeguards Rule

### General Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **G1** Develop a written information security plan. | | | |
| **G1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **G2** Designate one or more employees to coordinate the information security program. | | | |
| **G2** Examine information security policies and procedures to verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. | **Identify** **the information security policies** reviewed to verify the specific and formal assignment of the information security to a Chief Security Officer or other security-knowledgeable member of management. |  |  |
| **G3** Identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks. | | | |
| **G3.a** Verify that an annual risk-assessment process is documented that:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. | **Provide the name of the assessor** who attests that the documented annual risk-assessment process:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. |  |  |
| **G3.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | **Identify the risk assessment result documentation** reviewed to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. |  |  |
| **G4** Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information. | | | |
| **G4.a** Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom customer information is shared, or that could affect the security of customer information (for example, backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.), as follows: | **Identify the documented policies and procedures to manage service providers with whom customer information is shared, or that could affect the security of customer information**, reviewed to verify policy defines the following:   * Maintain a list of service providers. * Maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable GLBA requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s information, or manages the customer's network, applications or systems on behalf of a customer. * Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. |  |  |
| **G4.b** Verify that a list of service providers is maintained. | **Describe how** the documented list of service providers was observed to be maintained (kept up-to-date). |  |  |
| **G4.c** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of customer data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s network, applications or systems. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable GLBA requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer data, or manages the customer's network, applications or systems on behalf of a customer. |  |  |
| **G4.d** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Identify the policies and procedures** reviewed to verify that processes included proper due diligence prior to engaging any service provider. |  |  |
| **Describe how** it was observed that the above policies and procedures are implemented. |  |

### Employee Management and Training

|  |  |  |  |
| --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **E1** Check references or do background checks before hiring employees who will have access to customer information. | | | |
| **E1** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to customer data or the customer data environment. | **Identify the Human Resources personnel** interviewed who confirm background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to confidential data or the confidential data environment. |  |  |
| **Describe how** it was observed that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to confidential data or the confidential data environment. |  |
| **E2** Require every new employee to sign an agreement to follow your company’s confidentiality and security standards for handling customer information. | | | |
| **E2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. | **Describe how** it was verified that, per the security awareness program, all personnel: | |  |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  |
| * Provide an acknowledgement at least annually. |  |
| **E3** Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs. | | | |
| **E3** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | * **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **E4** Control access to sensitive information by requiring employees to use “strong” passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) | | | |
| **E4** For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | **Identify the sample** of system components selected for this testing procedure. |  |  |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that user password parameters are set to require at least the following strength/complexity: | |
| * Require a minimum length of at least seven characters. |  |
| * Contain both numeric and alphabetic characters. |  |
| **E5** Use password-activated screen savers to lock employee computers after a period of inactivity. | | | |
| **E5** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** **the sample** of system components selected for this testing procedure. |  |  |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that system/session idle time out features have been set to 15 minutes or less. |  |
| **E6** Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device. | | | |
| **E6** Verify that the usage policies define acceptable uses for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  |  |
| **E7** Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. | | | |
| **E7** Review the security awareness training documentation to verify it provides awareness to all personnel about the importance of protecting customer information. | **Identify** the documented security awareness training documentation reviewed to verify it includes at least the following topics:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. |  |  |
| **E8** Regularly remind all employees of your company’s policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms. | | | |
| **E8** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe** how the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **E9** Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions. | | | |
| **E9** Verify that telecommuting policies specify in detail at a minimum, the following:   * Whether or how employees are allowed to keep or access customer data at home * Requirement for employees who use personal computers or access cuistomer data to use adequate protection measures (anti-virus, firewall, patching, etc.) | **Identify** the documented telecommuting policy reviewed to verify it includes at least the following topics:   * Whether or how employees are allowed to keep or access customer data at home * Requirement for employees who use personal computers or access cuistomer data to use adequate protection measures (anti-virus, firewall, patching, etc.) |  |  |
| **E10** Impose disciplinary measures for security policy violations. | | | |
| **E10** Inquire with Human Resource department management and verify that employees are sanctioned when they violate security policies. | **Identify** the Human Resources personnel interviewed who confirm that employees are sanctioned when they violate security policies. |  |  |
| **E11** Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures. | | | |
| **E11.a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** the sample of users terminated in the past six months selected. |  |  |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **E11.b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  |  |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  |

### Information Systems

|  |  |  |  |
| --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **I1** Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods. | | | |
| **I1** Verify the existence of environmental security controls for each computer room, data center, and other storage areas containing customer data. | **Identify and briefly describe** all of the storage areas containing customer data: | |  |
| All computer rooms |  |
| All data centers |  |
| Any other physical areas |  |
| *For each identified area, complete the following*: | |
| Describe the environmental security controls to be in place |  |
| **I2** Store records in a room or cabinet that is locked when unattended. | | | |
| **I2** Observe the storage location’s physical security to confirm that all records storage is secure. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  |  |
| **I3** When customer information is stored on a server or other computer, ensure that the computer is accessible only with a “strong” password and is kept in a physically-secure area. | | | |
| **I3** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the customer data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. * Observe a system administrator’s attempt to log into consoles for randomly selected systems in the customer data environment and verify that they are “locked” to prevent unauthorized use. | **Identify and briefly describe** all of the storage areas containing customer data: | |  |
| All computer rooms |  |
| All data centers |  |
| Any other physical areas |  |
| *For each identified area, complete the following*: |  |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **Identify** the randomly selected systems in the confidential data environment for which a system administrator login attempt was observed. |  |
| **Describe how** consoles for the randomly selected systems were observed to verify that they are “locked” when not in use to prevent unauthorized use. |  |
| **I4** Where possible, avoid storing sensitive customer data on a computer with an Internet connection. | | | |
| **I4** Verify that all systems that store sensitive customer data either do not have an Internet connection, or must (for business or technical reasons) have an Internet connection. | **Identify and briefly describe** all computers that store sensitive customer data and have an Internet connection. |  |  |
| *For each computer that stores sensitive consumer data and has an Internet connection,* complete the following: | |
| **Describe** the reason why the computer must have an Internet connection. |  |
| **I5** Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area. | | | |
| **I5.a** Observe the storage location’s physical security to confirm that backup media storage is secure.Verify that the storage location security is reviewed at least annually. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  |  |
| **I6** Maintain a careful inventory of your company’s computers and any other equipment on which customer information may be stored. | | | |
| **I6.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. | **Describe how** the system inventory was examined to verify that a list of hardware and software components is: | |  |
| * Maintained |  |
| * Includes a description of function/use for each |  |
| **I6.b** Interview personnel to verify the documented inventory is kept current. | **Identify** **the responsible personnel** interviewed who confirm that the documented inventory is kept current. |  |  |
| **I7** When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. | | | |
| **I7.a** Identify all locations where confidential data or other sensitive financial data is transmitted or received over open, public networks. Examine system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where confidential data or other sensitive financial data is transmitted or received over open, public networks. |  |  |
| **I7.b** Select and observe a sample of inbound and outbound transmissions as they occur to verify that all confidential data or other sensitive financial data is encrypted with strong cryptography during transit. | **Describe** the sample of inbound and outbound transmissions observed as they occurred. |  |  |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all confidential data is encrypted with strong cryptography during transit. |  |
| **I8** If you collect information online directly from customers, make secure transmission automatic. | | | |
| **I8** Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. | *For all instances where customer data Is transmitted or received over open, public networks,* **describe how** system configurations were observed to verify that the protocol is implemented: | |  |
| To use only secure configurations. |  |
| Does not support insecure versions or configurations. |  |
| **I9** If you must transmit sensitive data by email over the Internet, be sure to encrypt the data. | | | |
| **I9.a** If end-user messaging technologies are used to send sensitive data, observe processes for sending sensitive data and examine a sample of outbound transmissions as they occur to verify that sensitive data is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | **Identify** whether end-user messaging technologies are used to send confidential data. **(yes/no)** |  |  |
| *If “no,” mark the remainder of I9.a as “Not Applicable” and proceed to I9.b.*  *If “yes,” complete the following:* | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **Describe** the sample of outbound transmissions observed as they occurred to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **I9.b** Review written policies to verify the existence of a policy stating that unprotected sensitive data are not to be sent via end-user messaging technologies. | *If “no” at I9.a:* | |  |
| **Identify** the policy document that explicitly prohibits sensitive data from being sent via end-user messaging technologies under any circumstance. |  |
| *If “yes” at I9.a:* | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **I10** Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group. | | | |
| **I10.a** Verify that responsibility for records retention and disposal has been formally assigned. | Provide the name of the assessor who attests that responsibility for records retention and disposal has been formally assigned. |  |  |
| **I10.b** If an outside disposal company is used, verify that the company has been certified by a recognized industry group. | Provide the name of the assessor who attests that the company has been certified by a recognized industry group. |  |  |
| **I11** Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed. | | | |
| **I11** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | **Identify** personnel interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  |  |
| **Provide the name of the assessor** who attests that the procedures state that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. |  |
| **I12** Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information. | | | |
| **I12** Verify that confidential data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media. | **Describe how** confidential data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. |  |  |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify** the industry-accepted standards used. |  |

### Detecting and Managing System Failures

|  |  |  |  |
| --- | --- | --- | --- |
| **GLBA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **D1** Monitor the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses. | | | |
| **D1** Interview responsible personnel and observe processes to verify that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. | * **Identify** the responsible personnel interviewed who confirm that: * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  |  |
| **Describe** the processes observed to verify that: | |
| New security vulnerabilities are identified. |  |
| A risk ranking is assigned to vulnerabilities to include identification of all “high” risk and “critical” vulnerabilities. |  |
| Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  |
| Identify the outside sources used. |  |
| **D2** Check with software vendors regularly to get and install patches that resolve software vulnerabilities. | | | |
| **D2** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:   * That applicable critical vendor-supplied security patches are installed within one month of release. * All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). | **Identify** **the sample** of system components and related software selected for this testing procedure. |  |  |
| **Identify** the vendor security patch list reviewed. |  |
| *For each item in the sample,* **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify that: | |
| Applicable critical vendor-supplied security patches are installed within one month of release. |  |
| All applicable vendor-supplied security patches are installed within an appropriate time frame. |  |
| **D3** Use anti-virus and anti-spyware software that updates automatically. | | | |
| **D3.a** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components selected (including all operating system types commonly affected by malicious software). |  |  |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  |
| **D3.b** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | * **Identify** the vendor documentation reviewed to verify that anti-virus programs: * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| Detect all known types of malicious software, |  |
| Remove all known types of malicious software, and |  |
| Protect against all known types of malicious software. |  |
| **D3.c** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are configured to perform automatic updates. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are Configured to perform automatic updates. |  |  |
| **D4** Maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations. | | | |
| **D4** Examine firewall configurations to verify they are up-to-date. | **Describe how** firewall configurations were examined to verify the firewalls are up-to-date. |  |  |
| **D5** Regularly ensure that ports not used for your business are closed. | | | |
| **D5.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. | **Identify** the firewall and router configuration standards reviewed to verify they require a review of firewall rule sets at least every six months. |  |  |
| **D5.b** Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. | **Identify** the document(s) relating to rule set reviews that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets. |  |  |
| **Identify the responsible personnel interviewed** who confirm that rule sets are reviewed at least every six months for firewall and router rule sets. |  |
| **D6** Promptly pass along information and instructions to employees regarding any new security risks or possible breaches. | | | |
| **D6** Verify that that information and instructions are promptly passed along to employees regarding any new security risks or possible breaches. | Provide the name of the assessor who attests that information and instructions are promptly passed along to employees regarding any new security risks or possible breaches. |  |  |
| **D7** Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information. | | | |
| **D7.a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | * **Identify** the documented security policies and procedures examined to verify that procedures define reviewing the following at least daily, either manually or via log tools: * All security events. * Logs of all system components that store, process, or transmit confidential data and/or SAD, or that could impact the security of confidential data and/or SAD. * Logs of all critical system components. * Logs of all servers and system components that perform security functions. |  |  |
| Describe the manual or log tools used for daily review of logs. |  |
| **D7.b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | * **Identify** the personnel interviewed who confirm that the following are reviewed at least daily: * All security events. * Logs of all system components that store, process, or transmit confidential data, or that could impact the security of confidential data. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | |
| All security events. |  |
| Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. |  |
| Logs of all critical system components. |  |
| Logs of all servers and system components that perform security functions. |  |
| **D8** Use an up-to-date intrusion detection system to alert you of attacks. | | | |
| **D8** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | **Identify** the vendor document(s) examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques |  |  |
| **Describe how** IDS/IPS configurations were examined and compared to vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are: | |
| Configured per vendor instructions to ensure optimal protection. |  |
| Maintained per vendor instructions to ensure optimal protection. |  |
| Updated per vendor instructions to ensure optimal protection. |  |
| **D9** Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. | | | |
| **D9** Verify that in- and out-bound transfers of infortmation are monitored for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. | **Descibe how** processes were observed to Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. |  |  |
| **D10** Take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet. | | | |
| **D10** Verify that the incident response plan includes specific incident response procedures. | Provide the name of the assessor who attests that the incident response plan includes specific incident response procedures. |  |  |
| **D11** Preserve and review files or programs that may reveal how a breach occurred. | | | |
| **D11** Verify that the incident response plan includes evidence gathering and retention requirements. | Provide the name of the assessor who attests that the incident response plan includes evidence gathering and retention requirements. |  |  |
| **D12** If feasible and appropriate, bring in security professionals to help assess a breach as soon as possible. | | | |
| **D12** Verify that the incident response plan includes contact information for security professionals if feasible and appropriate to help assess a breach as soon as possible. | Provide the name of the assessor who attests that the incident response plan includes contact information for security professionals if feasible and appropriate to help assess a breach as soon as possible |  |  |
| **D13** Notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm. | | | |
| **D13** Verify that the incident response plan includes procedures for notifying consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm. | Provide the name of the assessor who attests that the incident response plan includes procedures for notifying consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm. |  |  |
| **D14** Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm. | | | |
| **D14** Verify that the incident response plan includes procedures for notifying law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm. | Provide the name of the assessor who attests that the incident response plan includes procedures for notifying law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm. |  |  |
| **D15** Notify the credit bureaus and other businesses that may be affected by the breach. | | | |
| **D15** Verify that the incident response plan includes procedures for notifying the credit bureaus and other businesses that may be affected by the breach. | Provide the name of the assessor who attests that the incident response plan includes procedures for notifying the credit bureaus and other businesses that may be affected by the breach. |  |  |
| **D16** Check to see if breach notification is required under applicable state law. | | | |
| **D16** Verify that the incident response plan includes analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). | Provide the name of the assessor who attests that the incident response plan includes analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). |  |  |

## HIPAA

### Administrative Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | Control Description | Control Effectiveness | Notes |
| 164.308(a)(1)(i) | Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. |  |  |
| 164.308(a)(1)(ii)(A) | Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. |  |  |
| 164.308(a)(1)(ii)(B) | Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). |  |  |
| 164.308(a)(1)(ii)(C) | Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. |  |  |
| 164.308(a)(1)(ii)(D) | Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. |  |  |
| 164.308(a)(2) | Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. |  |  |
| 164.308(a)(3)(i) | Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. |  |  |
| 164.308(a)(3)(ii)(A) | Authorization and/or Supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. |  |  |
| 164.308(a)(3)(ii)(B) | Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. |  |  |
| 164.308(a)(3)(ii)(C) | Termination Procedure (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. |  |  |
| 164.308(a)(4)(i) | Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. |  |  |
| 164.308(a)(4)(ii)(A) | Isolating Healthcare Clearinghouse Functions (R): If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. |  |  |
| 164.308(a)(4)(ii)(B) | Access Authorization (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. |  |  |
| 164.308(a)(4)(ii)(C) | Access Establishment and Modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. |  |  |
| 164.308(a)(5)(i) | Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management). |  |  |
| 164.308(a)(5)(ii)(A) | Security Reminders (A): Periodic security updates. |  |  |
| 164.308(a)(5)(ii)(B) | Protection from Malicious Software (A): Procedures for guarding against, detecting, and reporting malicious software. |  |  |
| 164.308(a)(5)(ii)(C) | Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies. |  |  |
| 164.308(a)(5)(ii)(D) | Password Management (A): Procedures for creating, changing, and safeguarding passwords. |  |  |
| 164.308(a)(6)(i) | Security Incident Procedures: Implement policies and procedures to address security incidents. |  |  |
| 164.308(a)(6)(ii) | Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. |  |  |
| 164.308(a)(7)(i) | Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. |  |  |
| 164.308(a)(7)(ii)(A) | Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. |  |  |
| 164.308(a)(7)(ii)(B) | Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data. |  |  |
| 164.308(a)(7)(ii)(C) | Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. |  |  |
| 164.308(a)(7)(ii)(D) | Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans. |  |  |
| 164.308(a)(7)(ii)(E) | Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components. |  |  |
| 164.308(a)(8) | Evaluation: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart. |  |  |
| 164.308(b)(1) | Business Associate Contracts and Other Arrangements: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a), that the business associate will appropriately safeguard the information. |  |  |
| 164.308(b)(4) | Written Contract or Other Arrangement (R): Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a). |  |  |

### Physical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | Description | Control Effectiveness | Notes |
| 164.310(a)(1) | Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. |  |  |
| 164.310(a)(2)(i) | Contingency Operations (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. |  |  |
| 164.310(a)(2)(ii) | Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. |  |  |
| 164.310(a)(2)(iii) | Access Control and Validation Procedures (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. |  |  |
| 164.310(a)(2)(iv) | Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). |  |  |
| 164.310(b) | Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. |  |  |
| 164.310(c) | Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users. |  |  |
| 164.310(d)(1) | Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. |  |  |
| 164.310(d)(2)(i) | Disposal (R): Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored. |  |  |
| 164.310(d)(2)(ii) | Media Reuse (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. |  |  |
| 164.310(d)(2)(iii) | Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore. |  |  |
| 164.310(d)(2)(iv) | Data Backup and Storage (A): Create a retrievable exact copy of electronic protected health information, when needed, before movement of equipment. |  |  |

### Technical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | Description | Control Effectiveness | Notes |
| 164.312(a)(1) | Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). |  |  |
| 164.312(a)(2)(i) | Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. |  |  |
| 164.312(a)(2)(ii) | Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. |  |  |
| 164.312(a)(2)(iii) | Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. |  |  |
| 164.312(a)(2)(iv) | Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. |  |  |
| 164.312(b) | Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. |  |  |
| 164.312(c)(1) | Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. |  |  |
| 164.312(c)(2) | Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. |  |  |
| 164.312(d) | Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. |  |  |
| 164.312(e)(1) | Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. |  |  |
| 164.312(e)(2)(i) | Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. |  |  |
| 164.312(e)(2)(ii) | Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. |  |  |

## HIPAA

### Administrative Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.308(a)(1)(i)** Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. | | | |
| **164.308(a)(1)(i)** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **164.308(a)(1)(ii)(A)** Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. | | | |
| **164.308(a)(1)(ii)(A)** Verify that an annual risk assessment process is documented that identifies assets, threats, vulnerabilities, and results in a formal risk assessment. | **Describe how** it was verified that an annual risk-assessment process is documented that: | |  |
| * Identifies critical assets, threats and vulnerabilities. |  |
| * Results in formal, documented analysis of risk. |  |
| **164.308(a)(1)(ii)(B)** Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | | | |
| **164.308(a)(1)(ii)(B)** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | * **Identify** the risk assessment result documentation reviewed to verify that: * The risk assessment process is performed at least annually. * The risk assessment is performed upon significant changes to the environment. * The documented risk assessment process was followed. |  |  |
| **164.308(a)(1)(ii)(C)** Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | | | |
| **164.308(a)(1)(ii)(C)** Inquire with Human Resource department management and verify that employees are sanctioned when they violate security policies. | **Identify** the Human Resources personnel interviewed who confirm that employees are sanctioned when they violate security policies. |  |  |
| **164.308(a)(1)(ii)(D)** Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | | | |
| **164.308(a)(1)(ii)(D).a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | * **Identify** the documented security policies and procedures examined to verify that procedures define reviewing the following at least daily, either manually or via log tools: * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| Describe the manual or log tools used for daily review of logs. |  |
| **164.308(a)(1)(ii)(D).b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | * **Identify** the personnel interviewed who confirm that the following are reviewed at least daily: * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | |
| All security events. |  |
| Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. |  |
| Logs of all critical system components. |  |
| Logs of all servers and system components that perform security functions. |  |
| **164.308(a)(2)** Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | | | |
| **164.308(a)(2)** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. | * Provide the name of the assessor who attests that responsibilities were verified to be formally assigned for: * Establishing security policies and procedures. * Documenting security policies and procedures. * Distributing security policies and procedures. |  |  |
| **164.308(a)(3)(i)** Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | | | |
| **164.308(a)(3)(i)** Examine written policy for access control, and verify that the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function. * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | * **Identify** the written policy for access control that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows: * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **164.308(a)(3)(ii)(A)** Authorization and/or Supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | | | |
| **164.308(a)(3)(ii)(A)** Select a sample of user IDs and compare with documented approvals to verify that:   * Documented approval exists for the assigned privileges. * The approval was by authorized parties. * That specified privileges match the roles assigned to the individual. | * **Identify** the sample of user IDs examined for this testing procedure. |  |  |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | |
| * Documented approval exists for the assigned privileges. |  |  |
| * The approval was by authorized parties. |  |
| * That specified privileges match the roles assigned to the individual. |  |
| **164.308(a)(3)(ii)(B)** Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | | | |
| **164.308(a)(3)(ii)(B)** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. | * **Identify** the sample of user IDs examined for this testing procedure. |  |  |
| * **Identify** the responsible management personnel interviewed who confirm that privileges assigned are based on that individual’s job classification and function. |  |
| * For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each user ID in the selected sample are based on an individual’s job classification and function. |  |
| **164.308(a)(3)(ii)(C)** Termination Procedure (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | | | |
| **164.308(a)(3)(ii)(C).a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** the sample of users terminated in the past six months selected. |  |  |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **164.308(a)(3)(ii)(C).b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  |  |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  |
| **164.308(a)(4)(i)** Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | | | |
| **164.308(a)(4)(i)** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | * **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **164.308(a)(4)(ii)(A)** Isolating Healthcare Clearinghouse Functions (R): If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | | | |
| **164.308(a)(4)(ii)(A)** | **Identify** whether the organization is a healthcare clearinghouse that is part of a larger organization. **(yes/no)** |  |  |
| *If “no,” mark the remainder of 164.308(a)(4)(ii)(A) as “Not Applicable”*  *If “yes,” complete the following:* | | |
| **Identify** the policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. |  |  |
| **164.308(a)(4)(ii)(C)** Access Establishment and Modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | | | |
| **164.308(a)(4)(ii)(C)** Confirm that access control systems are in place on all system components. | **Identify** vendor documentation examined. |  |  |
| **Describe how** system settings were examined with the vendor documentation to verify that access control systems are in place on all system components. |  |  |
| **164.308(a)(5)(i)** Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management). | | | |
| **164.308(a)(5)(i)** Review the security awareness training documentation to verify it provides awareness to all personnel about the importance of protecting customer information. | **Identify** the documented security awareness training documentation reviewed to verify it includes at least the following topics:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. |  |  |
| **164.308(a)(5)(ii)(A)** Security Reminders (A): Periodic security updates. | | | |
| **164.308(a)(5)(ii)(A)** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe** how the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **164.308(a)(5)(ii)(B)** Protection from Malicious Software (A): Procedures for guarding against, detecting, and reporting malicious software. | | | |
| **164.308(a)(5)(ii)(B).a** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components selected (including all operating system types commonly affected by malicious software). |  |  |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  |
| **164.308(a)(5)(ii)(B).b** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | * **Identify** the vendor documentation reviewed to verify that anti-virus programs: * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| Detect all known types of malicious software, |  |
| Remove all known types of malicious software, and |  |
| Protect against all known types of malicious software. |  |
| **164.308(a)(5)(ii)(B).c** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are configured to perform automatic updates. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are Configured to perform automatic updates. |  |  |
| **164.308(a)(5)(ii)(C)** Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies. | | | |
| **164.308(a)(5)(ii)(C).a** Verify access to all audit trails is logged. | For all items in the sample, **describe how** configuration settings were observed to verify access to all audit trails is logged. |  |  |
| **164.308(a)(5)(ii)(C).b** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | **Identify** the documented security policies and procedures examined to verify that procedures define following up on exceptions and anomalies identified during the review process. |  |  |
| **164.308(a)(5)(ii)(C).c** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. | **Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed. |  |  |
| **Identify** the personnel interviewed who confirm that follow-up to exceptions and anomalies is performed. |  |
| **164.308(a)(5)(ii)(D)** Password Management (A): Procedures for creating, changing, and safeguarding passwords. | | | |
| **164.308(a)(5)(ii)(D).a** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use. | **Identify** the documented password procedures examined to verify the procedures define that:   * First-time passwords must be set to a unique value for each user. * First-time passwords must be changed after the first use. * Reset passwords must be set to a unique value for each user. * Reset passwords must be changed after the first use. |  |  |
| **Describe how** security personnel were observed to: | |
| * Set first-time passwords to a unique value for each new user. |  |
| * Set first-time passwords to be changed after first use. |  |
| * Set reset passwords to a unique value for each existing user. |  |
| * Set reset passwords to be changed after first use. |  |
| **164.308(a)(5)(ii)(D).b** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. | **Identify** the document examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  |  |
| **Describe** the non-face-to-face methods used for requesting password resets. |  |
| **Describe how** security personnel were observed to verify that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  |
| **164.308(a)(6)(i)** Security Incident Procedures: Implement policies and procedures to address security incidents. | | | |
| **164.308(a)(6)(i)** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach. | **Identify** the documented incident response plan and related procedures examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows:   * Create the incident response plan to be implemented in the event of system breach. * Test the plan at least annually. * Designate specific personnel to be available on a 24/7 basis to respond to alerts:   24/7 incident monitoring  24/7 incident response   * Provide appropriate training to staff with security breach response responsibilities. * Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. * Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  |  |
| **164.308(a)(6)(ii)** Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | | | |
| **164.308(a)(6)(ii).a** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. | **Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. |  |  |
| **Describe how** processes were reviewed to verify that ***responding to*** alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. |  |
| **164.308(a)(6)(ii).b** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **Identify** the documented policy reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  |
| **Identify** the sample of responsible personnel interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **164.308(a)(7)(i)** Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | | | |
| **164.308(a)(7)(i)** Examine the contingency plan and related procedures to verify entity is prepared to respond immediately to an emergency. | **Identify** the documented contingency plan and related procedures examined to verify the entity is prepared to respond immediately to an emergency. |  |  |
| **164.308(a)(7)(ii)(A)** Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | | | |
| **164.308(a)(7)(ii)(A)** Examine the data backup plan and related procedures to verify entity is able to create and maintain retrievable exact copies of electronic protected health information. | **Identify** the documented data backup plan and related procedures to verify entity is able to create and maintain retrievable exact copies of electronic protected health information. |  |  |
| **164.308(a)(7)(ii)(B)** Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data. | | | |
| **164.308(a)(7)(ii)(B)** Examine the disaster recovery plan and related procedures to verify entity is able to restore any loss of data. | **Identify** the documented disaster recovery plan and related procedures to verify entity is able to restore any loss of data. |  |  |
| **164.308(a)(7)(ii)(C)** Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | | | |
| **164.308(a)(7)(ii)(C)** Examine the emergency mode operation plan and related procedures to verify entity is able to continue critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | **Identify** the documented emergency mode operation plan and related procedures to verify entity is able to continue critical business processes for protection of the security of electronic protected health information while operating in emergency mode. |  |  |
| **164.308(a)(7)(ii)(D)** Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans. | | | |
| **164.308(a)(7)(ii)(D)** Examine the contingency plan and related procedures to verify entity periodically tests and revises the contingency plan. | **Identify** the documented contingency plan and related procedures to verify entity periodically tests and revises the contingency plan. |  |  |
| **164.308(a)(7)(ii)(E)** Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components. | | | |
| **164.308(a)(7)(ii)(E)** Examine the document containing applications and data criticality analysis to verity entity assesses the relative criticality of specific applications and data in support of other contingency plan components. | **Identify** the document containing applications and data criticality analysis to verity entity assesses the relative criticality of specific applications and data in support of other contingency plan components. |  |  |
| **164.308(a)(8)** Evaluation: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart. | | | |
| **164.308(a)(8)** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | **Identify** the document reviewed to verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. |  |  |
| **Describe how** the information security policy was verified to be: | |
| * Reviewed at least annually. |  |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  |
| **164.308(b)(1)** Business Associate Contracts and Other Arrangements: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a), that the business associate will appropriately safeguard the information. | | | |
| **164.308(b)(1)** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Describe how** it was verified that the procedures for proper due diligence prior to engaging a service provider are implemented. |  |  |
| **164.308(b)(4)** Written Contract or Other Arrangement (R): Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a). | | | |
| **164.308(b)(4)** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of customer data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s network, applications or systems. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable GLBA requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer data, or manages the customer's network, applications or systems on behalf of a customer. |  |  |

### Physical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.310(a)(1)** Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | | | |
| **164.310(a)(1)** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. | **Identify and briefly describe** all of the storage areas containing protected health information: | |  |
| All computer rooms |  |
| All data centers |  |
| Any other physical areas |  |
| *For each identified area, complete the following*: | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **164.310(a)(2)(i)** Contingency Operations (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | | | |
| **164.310(a)(2)(i)** Examine the disaster recovery plan and/or emergency mode operation plan and related procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | **Identify** the documented disaster recovery plan and/or emergency mode operation plan and related procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. |  |  |
| **164.310(a)(2)(ii)** Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | | | |
| **164.310(a)(2)(ii)** Examine the facility security plan plan that describes how entity safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. | **Identify** the documented facility security plan plan that describes how entity safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. |  |  |
| **164.310(a)(2)(iii)** Access Control and Validation Procedures (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | | | |
| **164.310(a)(2)(iii).a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:   * Identifying new onsite personnel or visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | **Identify** the documented processes reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying new onsite personnel or visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  |  |
| **164.310(a)(2)(iii).b** Observe processes for identifying and distinguishing between onsite personnel and visitors to verify that:   * Visitors are clearly identified, and   It is easy to distinguish between onsite personnel and visitors. | **Describe how** processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that: | |  |
| * Visitors are clearly identified, and |  |
| * It is easy to distinguish between onsite personnel and visitors. |  |
| **164.310(a)(2)(iv)** Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | | | |
| **164.310(a)(2)(iv)** Review documented processes to verify that entity documents repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | **Identify** the documented processes to verify that entity documents repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). |  |  |
| **164.310(b)** Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | | | |
| **164.310(b)** Review documented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | **Identify** the documented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. |  |  |
| **164.310(c)** Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users. | | | |
| **164.310(c)** Verify that all workstations that access electronic protected health information are located in areas restricted authorized users. | **Describe how** it was observed that all workstations that access electronic protected health information are located in areas restricted authorized users. |  |  |
| **164.310(d)(1)** Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | | | |
| **164.310(d)(1)** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | **Identify** the documented policy to control distribution of media that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  |  |
| **Describe how** media distribution is controlled, including distribution to individuals. |  |
| **164.310(d)(2)(i)** Disposal (R): Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored. | | | |
| **164.310(d)(2)(i)** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media. | **Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. |  |  |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify** the industry-accepted standards used. |  |
| **164.310(d)(2)(ii)** Media Reuse (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. | | | |
| **164.310(d)(2)(ii)** Verify that cardholder data on electronic media is removed before the media are made available for reuse. | **Identify** the procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. |  |  |
| **164.310(d)(2)(iii)** Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | | | |
| **164.310(d)(2)(iii)** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | **Identify** responsible personnel interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |  |
| *For each item in the sample above,* **describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |
| **164.310(d)(2)(iv)** Data Backup and Storage (A): Create a retrievable exact copy of electronic protected health information, when needed, before movement of equipment. | | | |
| **164.310(d)(2)(iv)** Verify that before equipment is moved, a retrievable exact copy of electronic protected health information is created, when needed. | **Identify** responsible personnel interviewed who confirm that before equipment is moved, a retrievable exact copy of electronic protected health information is created, when needed. |  |  |

### Technical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.312(a)(1)** Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). | | | |
| **164.312(a)(1)** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | **Describe how** system settings were examined to verify that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  |  |
| **164.312(a)(2)(i)** Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. | | | |
| **164.312(a)(2)(i)** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data. | **Identify** the responsible administrative personnel interviewed for this testing procedure. |  |  |
| For the interview, **summarize the relevant details discussed** to confirm that all users are assigned a unique ID for access to system components or cardholder data. |  |
| **164.312(a)(2)(ii)** Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | | | |
| **164.312(a)(2)(ii)** Review documented processes to verify that entity can obtain necessary electronic protected health information during an emergency. | **Identify** the documented processes to verify that entity can obtain necessary electronic protected health information during an emergency. |  |  |
| **164.312(a)(2)(iii)** Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | | | |
| **164.312(a)(2)(iii)** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** the sample of system components selected for this testing procedure. |  |  |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that system/session idle time out features have been set to 15 minutes or less. |  |
| **164.312(a)(2)(iv)** Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. | | | |
| **164.312(a)(2)(iv)** Examine documentation about the system used to protect electronic protected health information, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the electronic protected health information is rendered unreadable using strong cryptography, with associated key-management processes and procedures. | **Identify** the documentation about the system used to protect the electronic protected health information examined. |  |  |
| **Briefly describe** the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the electronic protected health information. |  |
| **164.312(b)** Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | | | |
| **164.312(b)** Implement audit trails to link all access to system components to each individual user. | Identify the system administrator(s) interviewed who confirm that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. |  |  |
| **Describe how** audit trails were observed to verify the following: | |
| * Audit trails are enabled and active for system components. |  |
| * Access to system components is linked to individual users. |  |
| **164.312(c)(1)** Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | | | |
| **164.312(c)(1)** Implement controls to protect electronic protected health information from improper alteration or destruction. | Identify the system administrator(s) interviewed who confirm that controls have been implemented which protect electronic protected health information from improper alteration or destruction. |  |  |
| **164.312(c)(2)** Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | | | |
| **164.312(c)(2)** Verify all individual access to electronic protected health information is logged. | **Describe how** configuration settings were observed to verify all individual access to electronic protected health information is logged. |  |  |
| **164.312(d)** Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | | | |
| **164.312(d)** Review procedures and confirm they define processes for verifying that a person or entity seeking access to electronic protected health information is the one claimed. | **Identify** the written procedures for user identification management examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or electronic protected health information data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |
| **164.312(e)(1)** Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | | | |
| **164.312(e)(1).a** Identify all locations where electronic protected health information is transmitted or received over open, public networks. Examine system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where electronic protected health information is transmitted or received over open, public networks. |  |  |
| **164.312(e)(1).b** Select and observe a sample of inbound and outbound transmissions as they occur to verify that all electronic protected health information is encrypted with strong cryptography during transit. | **Describe** the sample of inbound and outbound transmissions observed as they occurred. |  |  |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all electronic protected health information is encrypted with strong cryptography during transit. |  |
| **164.312(e)(2)(i)** Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | | | |
| **164.312(e)(2)(i)** Verify all individual access to electronic protected health information is logged. | **Describe how** configuration settings were observed to verify all individual access to electronic protected health information is logged. |  |  |
| **164.312(e)(2)(ii)** Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | | | |
| **164.312(e)(2)(ii)** Examine documentation about the system used to protect electronic protected health information, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the electronic protected health information is rendered unreadable using strong cryptography, with associated key-management processes and procedures. | **Identify** the documentation about the system used to protect the electronic protected health information examined. |  |  |
| **Briefly describe** the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the electronic protected health information. |  |

## HIPAA

### Administrative Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.308(a)(1)(i)** Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. | | | |
| **164.308(a)(1)(i)** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **164.308(a)(1)(ii)(A)** Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. | | | |
| **164.308(a)(1)(ii)(A)** Verify that an annual risk assessment process is documented that identifies assets, threats, vulnerabilities, and results in a formal risk assessment. | **Provide the name of the assessor** who attests that the documented annual risk-assessment process:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. |  |  |
| **164.308(a)(1)(ii)(B)** Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | | | |
| **164.308(a)(1)(ii)(B)** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | **Review** risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. |  |  |
| **164.308(a)(1)(ii)(C)** Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | | | |
| **164.308(a)(1)(ii)(C)** Inquire with Human Resource department management and verify that employees are sanctioned when they violate security policies. | **Identify** the Human Resources personnel interviewed who confirm that employees are sanctioned when they violate security policies. |  |  |
| **164.308(a)(1)(ii)(D)** Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | | | |
| **164.308(a)(1)(ii)(D).a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | **Identify** the documented security policies and procedures examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| Describe the manual or log tools used for daily review of logs. |  |
| **164.308(a)(1)(ii)(D).b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events. * Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. * Logs of all critical system components. * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | **Identify** the personnel interviewed who confirm that the following are reviewed at least daily:   * All security events. * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. * Logs of all critical system components.   Logs of all servers and system components that perform security functions. |  |  |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | |
| All security events. |  |
| Logs of all system components that store, process, or transmit customer data, or that could impact the security of customer data. |  |
| Logs of all critical system components. |  |
| Logs of all servers and system components that perform security functions. |  |
| **164.308(a)(2)** Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | | | |
| **164.308(a)(2)** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security policies and procedures. * Documenting security policies and procedures. * Distributing security policies and procedures. |  |  |
| **164.308(a)(3)(i)** Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | | | |
| **164.308(a)(3)(i)** Examine written policy for access control, and verify that the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function. * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | **Identify** the written policy for access control that was examined to verify the policy incorporates:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **164.308(a)(3)(ii)(A)** Authorization and/or Supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | | | |
| **164.308(a)(3)(ii)(A)** Select a sample of user IDs and compare with documented approvals to verify that:   * Documented approval exists for the assigned privileges. * The approval was by authorized parties. * That specified privileges match the roles assigned to the individual. | **Identify** the sample of user IDs examined for this testing procedure. |  |  |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | |
| * Documented approval exists for the assigned privileges. |  |
| * The approval was by authorized parties. |  |
| * That specified privileges match the roles assigned to the individual. |  |
| **164.308(a)(3)(ii)(B)** Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | | | |
| **164.308(a)(3)(ii)(B)** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. | **Identify** the sample of user IDs examined for this testing procedure. |  |  |
| **Identify** the responsible management personnel interviewed who confirm that privileges assigned are based on that individual’s job classification and function. |  |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each user ID in the selected sample are based on an individual’s job classification and function. |  |
| **164.308(a)(3)(ii)(C)** Termination Procedure (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | | | |
| **164.308(a)(3)(ii)(C).a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** the sample of users terminated in the past six months selected. |  |  |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **164.308(a)(3)(ii)(C).b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  |  |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  |
| **164.308(a)(4)(i)** Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | | | |
| **164.308(a)(4)(i)** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **164.308(a)(4)(ii)(A)** Isolating Healthcare Clearinghouse Functions (R): If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | | | |
| **164.308(a)(4)(ii)(A)** | **Identify** whether the organization is a healthcare clearinghouse that is part of a larger organization. **(yes/no)** |  |  |
| *If “no,” mark the remainder of 164.308(a)(4)(ii)(A) as “Not Applicable”*  *If “yes,” complete the following:* | |
| **Identify** the policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. |  |
| **164.308(a)(4)(ii)(C)** Access Establishment and Modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | | | |
| **164.308(a)(4)(ii)(C)** Confirm that access control systems are in place on all system components. | **Identify** vendor documentation examined. |  |  |
| **Describe how** system settings were examined with the vendor documentation to verify that access control systems are in place on all system components. |  |
| **164.308(a)(5)(i)** Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management). | | | |
| **164.308(a)(5)(i)** Review the security awareness training documentation to verify it provides awareness to all personnel about the importance of protecting customer information. | **Identify** the documented security awareness training documentation reviewed to verify it includes at least the following topics:   * Locking rooms and file cabinets where records are kept; * Not sharing or openly posting employee passwords in work areas; * Encrypting sensitive customer information when it is transmitted electronically via public networks; * Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and * Reporting suspicious attempts to obtain customer information to designated personnel. |  |  |
| **164.308(a)(5)(ii)(A)** Security Reminders (A): Periodic security updates. | | | |
| **164.308(a)(5)(ii)(A)** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe** how the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **164.308(a)(5)(ii)(B)** Protection from Malicious Software (A): Procedures for guarding against, detecting, and reporting malicious software. | | | |
| **164.308(a)(5)(ii)(B).a** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components selected (including all operating system types commonly affected by malicious software). |  |  |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  |
| **164.308(a)(5)(ii)(B).b** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | **Identify** the vendor documentation reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| Detect all known types of malicious software, |  |
| Remove all known types of malicious software, and |  |
| Protect against all known types of malicious software. |  |
| **164.308(a)(5)(ii)(B).c** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are configured to perform automatic updates. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are Configured to perform automatic updates. |  |  |
| **164.308(a)(5)(ii)(C)** Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies. | | | |
| **164.308(a)(5)(ii)(C).a** Verify access to all audit trails is logged. | For all items in the sample, **describe how** configuration settings were observed to verify access to all audit trails is logged. |  |  |
| **164.308(a)(5)(ii)(C).b** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | **Identify** the documented security policies and procedures examined to verify that procedures define following up on exceptions and anomalies identified during the review process. |  |  |
| **164.308(a)(5)(ii)(C).c** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. | **Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed. |  |  |
| **Identify** the personnel interviewed who confirm that follow-up to exceptions and anomalies is performed. |  |
| **164.308(a)(5)(ii)(D)** Password Management (A): Procedures for creating, changing, and safeguarding passwords. | | | |
| **164.308(a)(5)(ii)(D).a** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use. | **Identify** the documented password procedures examined to verify the procedures define that:   * First-time passwords must be set to a unique value for each user. * First-time passwords must be changed after the first use. * Reset passwords must be set to a unique value for each user. * Reset passwords must be changed after the first use. |  |  |
| **Describe how** security personnel were observed to: | |
| * Set first-time passwords to a unique value for each new user. |  |
| * Set first-time passwords to be changed after first use. |  |
| * Set reset passwords to a unique value for each existing user. |  |
| * Set reset passwords to be changed after first use. |  |
| **164.308(a)(5)(ii)(D).b** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. | **Identify** the document examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  |  |
| **Describe** the non-face-to-face methods used for requesting password resets. |  |
| **Describe how** security personnel were observed to verify that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  |
| **164.308(a)(6)(i)** Security Incident Procedures: Implement policies and procedures to address security incidents. | | | |
| **164.308(a)(6)(i)** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach. | **Identify** the documented incident response plan and related procedures examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows:   * Create the incident response plan to be implemented in the event of system breach. * Test the plan at least annually. * Designate specific personnel to be available on a 24/7 basis to respond to alerts:   24/7 incident monitoring  24/7 incident response   * Provide appropriate training to staff with security breach response responsibilities. * Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. * Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  |  |
| **164.308(a)(6)(ii)** Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | | | |
| **164.308(a)(6)(ii).a** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. | **Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. |  |  |
| **Describe how** processes were reviewed to verify that ***responding to*** alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan. |  |
| **164.308(a)(6)(ii).b** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **Identify** the documented policy reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  |
| **Identify** the sample of responsible personnel interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **164.308(a)(7)(i)** Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | | | |
| **164.308(a)(7)(i)** Examine the contingency plan and related procedures to verify entity is prepared to respond immediately to an emergency. | **Identify** the documented contingency plan and related procedures examined to verify the entity is prepared to respond immediately to an emergency. |  |  |
| **164.308(a)(7)(ii)(A)** Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | | | |
| **164.308(a)(7)(ii)(A)** Examine the data backup plan and related procedures to verify entity is able to create and maintain retrievable exact copies of electronic protected health information. | **Identify** the documented data backup plan and related procedures to verify entity is able to create and maintain retrievable exact copies of electronic protected health information. |  |  |
| **164.308(a)(7)(ii)(B)** Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data. | | | |
| **164.308(a)(7)(ii)(B)** Examine the disaster recovery plan and related procedures to verify entity is able to restore any loss of data. | **Identify** the documented disaster recovery plan and related procedures to verify entity is able to restore any loss of data. |  |  |
| **164.308(a)(7)(ii)(C)** Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | | | |
| **164.308(a)(7)(ii)(C)** Examine the emergency mode operation plan and related procedures to verify entity is able to continue critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | **Identify** the documented emergency mode operation plan and related procedures to verify entity is able to continue critical business processes for protection of the security of electronic protected health information while operating in emergency mode. |  |  |
| **164.308(a)(7)(ii)(D)** Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans. | | | |
| **164.308(a)(7)(ii)(D)** Examine the contingency plan and related procedures to verify entity periodically tests and revises the contingency plan. | **Identify** the documented contingency plan and related procedures to verify entity periodically tests and revises the contingency plan. |  |  |
| **164.308(a)(7)(ii)(E)** Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components. | | | |
| **164.308(a)(7)(ii)(E)** Examine the document containing applications and data criticality analysis to verity entity assesses the relative criticality of specific applications and data in support of other contingency plan components. | **Identify** the document containing applications and data criticality analysis to verity entity assesses the relative criticality of specific applications and data in support of other contingency plan components. |  |  |
| **164.308(a)(8)** Evaluation: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart. | | | |
| **164.308(a)(8)** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | **Describe how** the information security policy was verified to be: | |  |
| * Reviewed at least annually. |  |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  |
| **164.308(b)(1)** Business Associate Contracts and Other Arrangements: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a), that the business associate will appropriately safeguard the information. | | | |
| **164.308(b)(1)** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Identify the policies and procedures** reviewed to verify that processes included proper due diligence prior to engaging any service provider. |  |  |
| **Describe how** it was observed that the above policies and procedures are implemented. |  |
| **164.308(b)(4)** Written Contract or Other Arrangement (R): Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a). | | | |
| **164.308(b)(4)** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of customer data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s network, applications or systems. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable GLBA requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer data, or manages the customer's network, applications or systems on behalf of a customer. |  |  |

### Physical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.310(a)(1)** Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | | | |
| **164.310(a)(1)** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the PHI data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. | **Identify and briefly describe** all of the storage areas containing protected health information: | |  |
| All computer rooms |  |
| All data centers |  |
| Any other physical areas |  |
| *For each identified area, complete the following*: | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **164.310(a)(2)(i)** Contingency Operations (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | | | |
| **164.310(a)(2)(i)** Examine the disaster recovery plan and/or emergency mode operation plan and related procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | **Identify** the documented disaster recovery plan and/or emergency mode operation plan and related procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. |  |  |
| **164.310(a)(2)(ii)** Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | | | |
| **164.310(a)(2)(ii)** Examine the facility security plan plan that describes how entity safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. | **Identify** the documented facility security plan plan that describes how entity safeguards the facility and the equipment therein from unauthorized physical access, tampering, and theft. |  |  |
| **164.310(a)(2)(iii)** Access Control and Validation Procedures (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | | | |
| **164.310(a)(2)(iii).a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:   * Identifying new onsite personnel or visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | **Identify** the documented processes reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying new onsite personnel or visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  |  |
| **164.310(a)(2)(iii).b** Observe processes for identifying and distinguishing between onsite personnel and visitors to verify that:   * Visitors are clearly identified, and   It is easy to distinguish between onsite personnel and visitors. | **Describe how** processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that: | |  |
| * Visitors are clearly identified, and |  |
| * It is easy to distinguish between onsite personnel and visitors. |  |
| **164.310(a)(2)(iv)** Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | | | |
| **164.310(a)(2)(iv)** Review documented processes to verify that entity documents repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | **Identify** the documented processes to verify that entity documents repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). |  |  |
| **164.310(b)** Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | | | |
| **164.310(b)** Review documented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | **Identify** the documented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. |  |  |
| **164.310(c)** Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users. | | | |
| **164.310(c)** Verify that all workstations that access electronic protected health information are located in areas restricted authorized users. | **Describe how** it was observed that all workstations that access electronic protected health information are located in areas restricted authorized users. |  |  |
| **164.310(d)(1)** Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | | | |
| **164.310(d)(1)** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | * **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  |  |
| **164.310(d)(2)(i)** Disposal (R): Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored. | | | |
| **164.310(d)(2)(i)** Verify that PHI data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media. | **Describe how** PHI data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. |  |  |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify** the industry-accepted standards used. |  |
| **164.310(d)(2)(ii)** Media Reuse (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. | | | |
| **164.310(d)(2)(ii)** Verify that PHI data on electronic media is removed before the media are made available for reuse. | **Identify** the procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. |  |  |
| **164.310(d)(2)(iii)** Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | | | |
| **164.310(d)(2)(iii)** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | **Identify** responsible personnel interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |  |
| *For each item in the sample above,* **describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |
| **164.310(d)(2)(iv)** Data Backup and Storage (A): Create a retrievable exact copy of electronic protected health information, when needed, before movement of equipment. | | | |
| **164.310(d)(2)(iv)** Verify that before equipment is moved, a retrievable exact copy of electronic protected health information is created, when needed. | **Identify** responsible personnel interviewed who confirm that before equipment is moved, a retrievable exact copy of electronic protected health information is created, when needed. |  |  |

### Technical Safeguards

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **164.312(a)(1)** Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). | | | |
| **164.312(a)(1)** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | **Describe how** system settings were examined to verify that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  |  |
| **164.312(a)(2)(i)** Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. | | | |
| **164.312(a)(2)(i)** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or PHI data. | * **Identify** **the responsible administrative personnel** interviewed who confirm that all users are assigned a unique ID for access to system components or PHI data. |  |  |
| **164.312(a)(2)(ii)** Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | | | |
| **164.312(a)(2)(ii)** Review documented processes to verify that entity can obtain necessary electronic protected health information during an emergency. | **Identify** the documented processes to verify that entity can obtain necessary electronic protected health information during an emergency. |  |  |
| **164.312(a)(2)(iii)** Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | | | |
| **164.312(a)(2)(iii)** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** the sample of system components selected for this testing procedure. |  |  |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that system/session idle time out features have been set to 15 minutes or less. |  |
| **164.312(a)(2)(iv)** Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. | | | |
| **164.312(a)(2)(iv)** Examine documentation about the system used to protect electronic protected health information, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the electronic protected health information is rendered unreadable using strong cryptography, with associated key-management processes and procedures. | **Identify** **the documentation** examined to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  |  |
| **164.312(b)** Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | | | |
| **164.312(b)** Implement audit trails to link all access to system components to each individual user. | Identify the system administrator(s) interviewed who confirm that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. |  |  |
| **Describe how** audit trails were observed to verify the following: | |
| * Audit trails are enabled and active for system components. |  |
| * Access to system components is linked to individual users. |  |
| **164.312(c)(1)** Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | | | |
| **164.312(c)(1)** Implement controls to protect electronic protected health information from improper alteration or destruction. | Identify the system administrator(s) interviewed who confirm that controls have been implemented which protect electronic protected health information from improper alteration or destruction. |  |  |
| **164.312(c)(2)** Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | | | |
| **164.312(c)(2)** Verify all individual access to electronic protected health information is logged. | **Describe how** configuration settings were observed to verify all individual access to electronic protected health information is logged. |  |  |
| **164.312(d)** Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | | | |
| **164.312(d)** Review procedures and confirm they define processes for verifying that a person or entity seeking access to electronic protected health information is the one claimed. | **Identify** the written procedures for user identification management examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or electronic protected health information data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |
| **164.312(e)(1)** Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | | | |
| **164.312(e)(1).a** Identify all locations where electronic protected health information is transmitted or received over open, public networks. Examine system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where electronic protected health information is transmitted or received over open, public networks. |  |  |
| **164.312(e)(1).b** Select and observe a sample of inbound and outbound transmissions as they occur to verify that all electronic protected health information is encrypted with strong cryptography during transit. | **Describe** the sample of inbound and outbound transmissions observed as they occurred. |  |  |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all electronic protected health information is encrypted with strong cryptography during transit. |  |
| **164.312(e)(2)(i)** Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | | | |
| **164.312(e)(2)(i)** Verify all individual access to electronic protected health information is logged. | **Describe how** configuration settings were observed to verify all individual access to electronic protected health information is logged. |  |  |
| **164.312(e)(2)(ii)** Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | | | |
| **164.312(e)(2)(ii)** Examine documentation about the system used to protect electronic protected health information, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the electronic protected health information is rendered unreadable using strong cryptography, with associated key-management processes and procedures. | **Identify** **the documentation** examined to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  |  |

## ISO 27002

### A.5 Security Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 5.1 Information Security Policy | | | | |
| 5.1.1 | Information security policy document | An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. |  |  |
| 5.1.2 | Review of the information security policy | The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. |  |  |

### A.6 Organization of Information Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 6.1 Internal Organization | | | | |
| 6.1.1 | Management commitment to information security | Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. |  |  |
| 6.1.2 | Information security co-ordination | Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. |  |  |
| 6.1.3 | Allocation of information security responsibilities | All information security responsibilities should be clearly defined. |  |  |
| 6.1.4 | Authorization process for information processing facilities | A management authorization process for new information processing facilities should be defined and implemented. |  |  |
| 6.1.5 | Confidentiality agreements | Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified and regularly reviewed. |  |  |
| 6.1.6 | Contact with authorities | Appropriate contacts with relevant authorities should be maintained. |  |  |
| 6.1.7 | Contact with special interest groups | Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. |  |  |
| 6.1.8 | Independent review of information security | The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur. |  |  |
| 6.2 External Parties | | | | |
| 6.2.1 | Identification of risks related to external parties | The risks to the organization’s information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. |  |  |
| 6.2.2 | Addressing security when dealing with customers | All identified security requirements should be addressed before giving customers access to the organization’s information or assets. |  |  |
| 6.2.3 | Addressing security in third party agreements | Agreements with third parties involving accessing, processing, communicating or managing the organization’s information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements. |  |  |

### A.7 Asset Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 7.1 Responsibility for Assets | | | | |
| 7.1.1 | Inventory of assets | All assets should be clearly identified and an inventory of all important assets drawn up and maintained. |  |  |
| 7.1.2 | Ownership of assets | All information and assets associated with information processing facilities should be owned by a designated part of the organization. |  |  |
| 7.1.3 | Acceptable use of assets | Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented. |  |  |
| 7.2 Information Classification | | | | |
| 7.2.1 | Classification Guidelines | Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. |  |  |
| 7.2.2 | Information labeling and handling | An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. |  |  |

### A.8 Human Resources Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 8.1 Prior to Employment | | | | |
| 8.1.1 | Roles and Responsibilities | Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization’s information security policy. |  |  |
| 8.1.2 | Screening | Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. |  |  |
| 8.1.3 | Terms and conditions of employment | As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization’s responsibilities for information security. |  |  |
| 8.2 During Employment | | | | |
| 8.2.1 | Management responsibilities | Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. |  |  |
| 8.2.2 | Awareness, education, and training | All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. |  |  |
| 8.2.3 | Disciplinary process | There should be a formal disciplinary process for employees who have committed a security breach. |  |  |
| 8.3 Termination or change of employment | | | | |
| 8.3.1 | Termination responsibilities | Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. |  |  |
| 8.3.2 | Return of assets | All employees, contractors and third party users should return all of the organization’s assets in their possession upon termination of their employment, contract or agreement. |  |  |
| 8.3.3 | Removal of access rights | The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. |  |  |

### A.9 Physical and Environmental Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 9.1 Secure areas | | | | |
| 9.1.1 | Physical security perimeter | Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities. |  |  |
| 9.1.2 | Physical entry controls | Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. |  |  |
| 9.1.3 | Securing offices, rooms, facilities | Physical security for offices, rooms, and facilities should be designed and applied. |  |  |
| 9.1.4 | Protecting against external and environmental threats | Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. |  |  |
| 9.1.5 | Working in secure areas | Physical protection and guidelines for working in secure areas should be designed and applied. |  |  |
| 9.1.6 | Public access, delivery and loading areas | Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. |  |  |
| 9.2 Equipment security | | | | |
| 9.2.1 | Equipment siting and protection | Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |  |  |
| 9.2.2 | Supporting utilities | Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |
| 9.2.3 | Cabling security | Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. |  |  |
| 9.2.4 | Equipment maintenance | Equipment should be correctly maintained to ensure its continued availability and integrity. |  |  |
| 9.2.5 | Security of equipment off-premises | Security should be applied to off-site equipment taking into account the different risks of working outside the organization’s premises. |  |  |
| 9.2.6 | Secure disposal or reuse of equipment | All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. |  |  |
| 9.2.7 | Removal of property | Equipment, information or software should not be taken off-site without prior authorization. |  |  |

### A.10 Communications and Operations Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 10.1 Operational procedures and responsibilities | | | | |
| 10.1.1 | Documented operating procedures | Operating procedures should be documented, maintained, and made available to all users who need them. |  |  |
| 10.1.2 | Change management | Changes to information processing facilities and systems should be controlled. |  |  |
| 10.1.3 | Segregation of duties | Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. |  |  |
| 10.1.4 | Separation of development, test and operational facilities | Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system. |  |  |
| 10.2 Service delivery | | | | |
| 10.2.1 | Service delivery | It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. |  |  |
| 10.2.2 | Monitoring and review of third-party services | The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly. |  |  |
| 10.2.3 | Managing changes to third-party services | Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks. |  |  |
| 10.3 System planning and acceptance | | | | |
| 10.3.1 | Capacity management | The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. |  |  |
| 10.3.2 | System acceptance | Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. |  |  |
| 10.4 Protection against malicious and mobile code | | | | |
| 10.4.1 | Controls against malicious code | Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. |  |  |
| 10.4.2 | Controls against mobile code | Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing. |  |  |
| 10.5 Backup | | | | |
| 10.5.1 | Information Backup | Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy. |  |  |
| 10.6 Network security management | | | | |
| 10.6.1 | Network controls | Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. |  |  |
| 10.6.2 | Security of network services | Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced. |  |  |
| 10.7 Media handling | | | | |
| 10.7.1 | Management of removable media | There should be procedures in place for the management of removable media. |  |  |
| 10.7.2 | Disposal of media | Media should be disposed of securely and safely when no longer required, using formal procedures. |  |  |
| 10.7.3 | Information handling procedures | Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse. |  |  |
| 10.7.4 | Security of system documentation | System documentation should be protected against unauthorized access. |  |  |
| 10.8 Exchange of information | | | | |
| 10.8.1 | Information exchange policies and procedures | Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. |  |  |
| 10.8.2 | Exchange agreements | Agreements should be established for the exchange of information and software between the organization and external parties. |  |  |
| 10.8.3 | Physical media in transit | Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization’s physical boundaries. |  |  |
| 10.8.4 | Electronic messaging | Information involved in electronic messaging should be appropriately protected. |  |  |
| 10.8.5 | Business information systems | Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems. |  |  |
| 10.9 Electronic commerce services | | | | |
| 10.9.1 | Electronic commerce | Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. |  |  |
| 10.9.2 | Online transactions | Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. |  |  |
| 10.9.3 | Publicly available information | The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification. |  |  |
| 10.10 Monitoring | | | | |
| 10.10.1 | Audit logging | Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. |  |  |
| 10.10.2 | Monitoring system use | Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. |  |  |
| 10.10.3 | Protection of log information | Logging facilities and log information should be protected against tampering and unauthorized access. |  |  |
| 10.10.4 | Administrator and operator logs | System administrator and system operator activities should be logged. |  |  |
| 10.10.5 | Fault logging | Faults should be logged, analyzed, and appropriate action taken. |  |  |
| 10.10.6 | Clock synchronization | The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source. |  |  |

### A.11 Access Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 11.1 Business requirement for access control | | | | |
| 11.1.1 | Access control policy | An access control policy should be established, documented, and reviewed based on business and security requirements for access. |  |  |
| 11.2 User access management | | | | |
| 11.2.1 | User registration | There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. |  |  |
| 11.2.2 | Privilege management | The allocation and use of privileges should be restricted and controlled. |  |  |
| 11.2.3 | User password management | The allocation of passwords should be controlled through a formal management process. |  |  |
| 11.2.4 | Review of user access rights | Management should review users’ access rights at regular intervals using a formal process. |  |  |
| 11.3 User responsibilities | | | | |
| 11.3.1 | Password use | Users should be required to follow good security practices in the selection and use of passwords. |  |  |
| 11.3.2 | Unattended user equipment | Users should ensure that unattended equipment has appropriate protection. |  |  |
| 11.3.3 | Clear desk and clear screen policy | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. |  |  |
| 11.4 Network access control | | | | |
| 11.4.1 | Policy on use of network services | Users should only be provided with access to the services that they have been specifically authorized to use. |  |  |
| 11.4.2 | User authentication for external connections | Appropriate authentication methods should be used to control access by remote users. |  |  |
| 11.4.3 | Equipment identification in networks | Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. |  |  |
| 11.4.4 | Remote diagnostic and configuration port protection | Physical and logical access to diagnostic and configuration ports should be controlled. |  |  |
| 11.4.5 | Segregation in networks | Groups of information services, users, and information systems should be segregated on networks. |  |  |
| 11.4.6 | Network connection control | For shared networks, especially those extending across the organization’s boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1). |  |  |
| 11.4.7 | Network routing control | Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. |  |  |
| 11.5 Operating system access control | | | | |
| 11.5.1 | Secure log-on procedures | Access to operating systems should be controlled by a secure log-on procedure. |  |  |
| 11.5.2 | User identification and authentication | All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. |  |  |
| 11.5.3 | Password management system | Systems for managing passwords should be interactive and should ensure quality passwords. |  |  |
| 11.5.4 | Use of system utilities | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. |  |  |
| 11.5.5 | Session time-out | Inactive sessions should shut down after a defined period of inactivity. |  |  |
| 11.5.6 | Limitation of connection time | Restrictions on connection times should be used to provide additional security for high-risk applications. |  |  |
| 11.6 Application and information access control | | | | |
| 11.6.1 | Information access restriction | Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. |  |  |
| 11.6.2 | Sensitive system isolation | Sensitive systems should have a dedicated (isolated) computing environment. |  |  |
| 11.7 Mobile computing and teleworking | | | | |
| 11.7.1 | Mobile computing and communications | A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities. |  |  |
| 11.7.2 | Teleworking | A policy, operational plans and procedures should be developed and implemented for teleworking activities. |  |  |

### A.12 Information Systems Acquisition, Development and Maintenance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 12.1 Security requirements of information systems | | | | |
| 12.1.1 | Security requirements analysis and specification | Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls. |  |  |
| 12.2 Correct processing in applications | | | | |
| 12.2.1 | Input data validation | Data input to applications should be validated to ensure that this data is correct and appropriate. |  |  |
| 12.2.2 | Control of internal processing | Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. |  |  |
| 12.2.3 | Message integrity | Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented. |  |  |
| 12.2.4 | Output data validation | Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. |  |  |
| 12.3 Cryptographic controls | | | | |
| 12.3.1 | Policy on the use of cryptographic controls | A policy on the use of cryptographic controls for protection of information should be developed and implemented. |  |  |
| 12.3.2 | Key management | Key management should be in place to support the organization’s use of cryptographic techniques. |  |  |
| 12.4 Security of system files | | | | |
| 12.4.1 | Control of operational software | There should be procedures in place to control the installation of software on operational systems. |  |  |
| 12.4.2 | Protection of system test data | Test data should be selected carefully, and protected and controlled. |  |  |
| 12.4.3 | Access control to program source code | Access to program source code should be restricted. |  |  |
| 12.5 Security in development and support processes | | | | |
| 12.5.1 | Change control procedures | The implementation of changes should be controlled by the use of formal change control procedures. |  |  |
| 12.5.2 | Technical review of applications after operating system changes | When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. |  |  |
| 12.5.3 | Restrictions on changes to software packages | Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled. |  |  |
| 12.5.4 | Information leakage | Opportunities for information leakage should be prevented. |  |  |
| 12.5.5 | Outsourced software development | Outsourced software development should be supervised and monitored by the organization. |  |  |
| 12.6 Technical Vulnerability Management | | | | |
| 12.6.1 | Control of technical vulnerabilities | Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. |  |  |

### A.13 Information Security Incident Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 13.1 Reporting information security events and weaknesses | | | | |
| 13.1.1 | Reporting information security events | Information security events should be reported through appropriate management channels as quickly as possible. |  |  |
| 13.1.2 | Reporting security weaknesses | All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services. |  |  |
| 13.2 Management of information security incidents and improvements | | | | |
| 13.2.1 | Responsibilities and procedures | Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. |  |  |
| 13.2.2 | Learning from information security incidents | There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. |  |  |
| 13.2.3 | Collection of evidence | Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). |  |  |

### A.14 Business Continuity Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 14.1 Information security aspects of business continuity management | | | | |
| 14.1.1 | Including information security in the business continuity management process | A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity. |  |  |
| 14.1.2 | Business continuity and risk assessment | Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. |  |  |
| 14.1.3 | Developing and implementing continuity plans including information security | Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. |  |  |
| 14.1.4 | Business continuity planning framework | A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. |  |  |
| 14.1.5 | Testing, maintaining and reassessing business continuity plans | Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective. |  |  |

### A.15 Compliance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 15.1 Compliance with legal requirements | | | | |
| 15.1.1 | Identification of applicable legislation | All relevant statutory, regulatory, and contractual requirements and the organization’s approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. |  |  |
| 15.1.2 | Intellectual property rights (IPR) | Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. |  |  |
| 15.1.3 | Protection of organizational records | Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. |  |  |
| 15.1.4 | Data protection and privacy of personal information | Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. |  |  |
| 15.1.5 | Prevention of misuse of information processing facilities | Users should be deterred from using information processing facilities for unauthorized purposes. |  |  |
| 15.1.6 | Regulation of cryptographic controls | Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. |  |  |
| 15.2 Compliance with security policies and standards, and technical compliance | | | | |
| 15.2.1 | Compliance with security policies and standards | Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. |  |  |
| 15.2.2 | Technical compliance checking | Information systems should be regularly checked for compliance with security implementation standards. |  |  |
| 15.3 Information systems audit considerations | | | | |
| 15.3.1 | Information systems audit controls | Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. |  |  |
| 15.3.2 | Protection of information systems audit tools | Access to information systems audit tools should be protected to prevent any possible misuse or compromise. |  |  |

## ISO 27002

### A.5 Information Security Policies

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **5.1 Management Direction for Information Security** | | | |
| **5.1.1** Information security policy document. | | | |
| An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **5.1.2** Review of the policies for information security. | | | |
| The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | **Identify** **the information security policies** reviewed to verify the specific and formal assignment of the information security to a Chief Security Officer or other security-knowledgeable member of management. |  |  |

### A.6 Organization of Information Security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **6.1 Internal organization** | | | |
| **6.1.1** Information security roles and responsibilities | | | |
| All information security responsibilities should be defined and allocated. | **Identify the documented policy** reviewed to verify all information security responsibilities should be defined and allocated. |  |  |
| **6.1.2** Segregation of duties | | | |
| Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. | **Identify the documented policy** reviewed to verify responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. |  |  |
| **6.1.3** Contact with authorities | | | |
| Appropriate contacts with relevant authorities should be maintained. | **Identify the documented policy** reviewed to verify appropriate contacts with relevant authorities should be maintained. |  |  |
| **6.1.4** Contact with special interest groups | | | |
| Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. | **Identify the documented policy** reviewed to verify appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. |  |  |
| **6.1.5** Information security in project management | | | |
| Information security should be addressed in project management, regardless of the type of the project. | **Identify** the personnel interviewed to confirm that Information Security is addressed in project management. |  |  |
| **6.2**  **Mobile devices and teleworking** | | | |
| **6.2.1** Mobile device policy | | | |
| A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices. | **Indicate whether** mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network are used to access the organization’s network. **(yes/no)** |  |  |
| *If “no,”* **identify** **the document** reviewed that explicitly prohibits mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network from being used to access the organization’s network. |  |
| *If “yes,”* **identify** **the documented policies and configuration standards** that define the following:   * Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network, and which are also used to access the network. * Specific configuration settings are defined for personal firewall software. * Personal firewall software is configured to actively run. * Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. |  |
| **6.2.2** Teleworking | | | |
| A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. | **Identify the documented policy** reviewed to verify policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. |  |  |

### A.7 Human resources security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **7.1 Prior to employment** | | | |
| **7.1.1** Screening | | | |
| Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | **Identify the documented policy** reviewed to verify requirement for background checks to be conducted:   * On potential personnel who will have access to the environment. * Prior to hiring the personnel. |  |  |
| **Identify the Human Resources personnel** interviewed who confirm background checks are conducted:   * On potential personnel who will have access to environment. * Prior to hiring the personnel. |  |
| **Describe how** it was verified that background checks are conducted (within the constraints of local laws): | |
| * On potential personnel who will have access to the environment. |  |
| * Prior to hiring the personnel. |  |
| **7.1.2** Terms and conditions of employment | | | |
| The contractual agreements with employees and contractors should state their and the organization’s responsibilities for information security. | **Describe how** it was verified that, per the security awareness program, all personnel: | |  |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  |
| * Provide an acknowledgement at least annually. |  |
| **7.2 During employment** | | | |
| **7.2.1** Management responsibilities | | | |
| Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. | **Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **7.2.2** Information security awareness, education and training | | | |
| All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. | **Identify the documented security awareness program** reviewed to verify it provides awareness to all personnel about the importance of confidential data security. |  |  |
| **Identify the documented security awareness program procedures and additional documentation** examined to verify that:   * The security awareness program provides multiple methods of communicating awareness and educating personnel. * Personnel attend security awareness training: * Upon hire, and * At least annually * Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. |  |
| **7.2.3** Disciplinary process | | | |
| There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. | **Identify the documented policy** reviewed to verify appropriate contacts with relevant authorities should be maintained. |  |  |
| **7.3 Termination and change of employment** | | | |
| **7.3.1** Termination or change of employment responsibilities | | | |
| Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. | **Identify the documented policy** reviewed to verify responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. |  |  |

### A.8 Asset management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **8.1 Responsibility for assets** | | | |
| **8.1.1** Inventory of assets | | | |
| Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. | **Describe how** the system inventory was examined to verify that a list of hardware and software components is: | |  |
| * Maintained |  |
| * Includes a description of function/use for each |  |
| **8.1.2** Ownership of assets | | | |
| Assets maintained in the inventory should be owned. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.1.3** Acceptable use of assets | | | |
| Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  |  |
| **8.1.4** Return of assets | | | |
| All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.2 Information classification** | | | |
| **8.2.1** Classification of information | | | |
| Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. | **Identify the documented policy** reviewed to verify Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. |  |  |
| **8.2.2** Labelling of information | | | |
| An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization. | **Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine:   * Owner * Contact Information * Purpose   (for example,labeling, coding, and/or inventorying of devices). |  |  |
| **8.2.3** Handling of assets | | | |
| Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.3 Media handling** | | | |
| **8.3.1** Management of removable media | | | |
| Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. | **Identify the documented policy** reviewed to verify policy defines how media is classified. |  |  |
| **Describe how** the classifications were observed to be implemented so the sensitivity of the data can be determined. |  |
| **8.3.2** Disposal of media | | | |
| Media should be disposed of securely when no longer required, using formal procedures. | **Identify** **personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  |  |
| **Describe how** the procedures were examined to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. |  |
| **8.3.3** Physical media transfer | | | |
| Media containing information should be protected against unauthorized access, misuse or corruption during transportation. | **Identify** **responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |  |
| **Describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |

### A.9 Access Control

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **9.1 Business requirements of access control** | | | |
| **9.1.1** Access control policy | | | |
| An access control policy should be established, documented and reviewed based on business and information security requirements. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function   Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.1.2** Access to networks and network services | | | |
| Users should only be provided with access to the network and network services that they have been specifically authorized to use. | **Identify the sample** of user IDs examined for this testing procedure. |  |  |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | |
| * Documented approval exists for the assigned privileges. |  |
| * The approval was by authorized parties. |  |
| * That specified privileges match the roles assigned to the individual. |  |
| **9.2 User access management** | | | |
| **9.2.1** User registration and de-registration | | | |
| A formal user registration and de-registration process should be implemented to enable assignment of access rights. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function   Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.2.2** User access provisioning | | | |
| A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services. | **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **9.2.3** Management of privileged access rights | | | |
| The allocation and use of privileged access rights should be restricted and controlled. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.2.4** Management of secret authentication information for users | | | |
| The allocation of secret authentication information should be controlled through a formal management process. | **Identify** **the document** that contains the management of secret authentication information for users. |  |  |
| **9.2.5** Review of user access rights | | | |
| Asset owners should review users’ access rights at regular intervals. | **Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled and user rights are reviewed. |  |  |
| **9.2.6** Removal or adjustment of user access rights | | | |
| The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. | **Identify** **the sample** of users terminated in the past six months selected. |  |  |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **9.3 User responsibilities** | | | |
| **9.3.1** User of secret authentication information | | | |
| Users should be required to follow the organization’s practices in the use of secret authentication information. | **Identify** **the document** that contains the management of secret authentication information for users. |  |  |
| **9.4 System and application access control** | | | |
| **9.4.1** Information access restriction | | | |
| Access to information and application system functions should be restricted in accordance with the access control policy. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates:   * Access to information and application system. |  |  |
| **9.4.2** Secure log-on procedures | | | |
| Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure. | **Identify** all applications containing confidential data. |  |  |
| **Describe how** authentication is managed (for example, via application and/or database interfaces). |  |
| **Describe how** database and/or application configuration settings were observed to verify that all users are authenticated prior to access. |  |
| **9.4.3** Password management system | | | |
| Password management systems should be interactive and should ensure quality passwords. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8:   * Assign all users a unique ID before allowing them to access system components or confidential data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |
| **9.4.4** Use of privileged utility programs | | | |
| The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | **Identify the assessor** who attests that users cannot installed software or utility programs and that they are tightly controlled. |  |  |
| **9.4.5** Access control to program source code | | | |
| Access to program source code should be restricted. | **Identify the assessor** who attests that access to program source code is restricted. |  |  |

### A.10 Cryptography

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **10.1 Cryptographic controls** | | | |
| **10.1.1** Policy on the use of cryptographic controls | | | |
| A policy on the use of cryptographic controls for protection of information should be developed and implemented. | **Identify** **the documentation** examined about the system used to protect the confidential information. |  |  |
| **Briefly describe** the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the confidential information. |  |
| **Identify** which of the following methods is used to render the confidential information unreadable:   * One-way hashes based on strong cryptography * Truncation * Index token and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  |
| **10.1.2** Key management | | | |
| A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle. | **Identify** **the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of confidential data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys.   Keys are stored securely in the fewest possible locations and forms. |  |  |

### A.11 Physical and environmental security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **11.1 Secure areas** | | | |
| **11.1.1** Physical security perimeter | | | |
| Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. | **Identify and briefly describe** all of the following with systems in the confidential data environment: | |  |
| * All computer rooms |  |
| * All data centers |  |
| * Any other physical areas |  |
| *For each area identified (add rows as needed),* complete the following: | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **Identify** the randomly selected systems in the confidential environment for which a system administrator login attempt was observed. |  |
| **Describe how** consoles for the randomly selected systems were observed to verify that they are “locked” when not in use to prevent unauthorized use. |  |
| **11.1.2** Physical entry controls | | | |
| Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. | **Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access. |  |  |
| **11.1.3** Securing offices, rooms, facilities | | | |
| Physical security for offices, rooms and facilities should be designed and applied. | **Describe** the video cameras and/or access control mechanisms observed to monitor the entry/exit points to office and sensitive areas. |  |  |
| **11.1.4** Protecting against external and environmental threats | | | |
| Physical protection against natural disasters, malicious attack or accidents should be designed and applied. | **Identify the documented**  **Business Continuity and Disaster Recovery Policy to show** Protecting against external and environmental threats |  |  |
| **11.1.5** Working in secure areas | | | |
| Procedures for working in secure areas should be designed and applied. | **Identify** **the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  |  |
| **11.1.6** Delivery and loading areas | | | |
| Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. | **Describe** how access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. |  |  |
| **11.2 Equipment** | | | |
| **11.2.1** Equipment siting and protection | | | |
| Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. | **Identify** **the assessor who confirms e**quipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |  |  |
| **11.2.2** Supporting utilities | | | |
| Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. | **Identify** **the assessor who confirms** Equipment is protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |
| **11.2.3** Cabling security | | | |
| Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage. | **Identify** **the assessor who confirms** power and telecommunications cabling carrying data or supporting information services is protected from interception, interference or damage. |  |  |
| **11.2.4** Equipment maintenance | | | |
| Equipment should be correctly maintained to ensure its continued availability and integrity. | **Identify** **the assessor who confirms** equipment is correctly maintained to ensure its continued availability and integrity. |  |  |
| **11.2.5** Removal of assets | | | |
| Equipment, information or software should not be taken off-site without prior authorization. | **Identify** **the assessor who confirms e**quipment, information or software is not taken off-site without prior authorization. |  |  |
| **11.2.6** Security of equipment and assets off-premises | | | |
| Security should be applied to off-site assets taking into account the different risks of working outside the organization’s. premises | **Identify** **the assessor who confirms** security is applied to off-site assets taking into account the different risks of working outside the organization’s premises. |  |  |
| **11.2.7** Secure disposal or re-use of equipment | | | |
| All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. | **Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Confidential data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). |  |  |
| **11.2.8** Unattended user equipment | | | |
| Users should ensure that unattended equipment has appropriate protection. | **Identify** **all locations** where backup media is stored. |  |  |
| **Describe how** it was observed that backup media storage is stored in a secure location. |  |
| **11.2.9** Clear desk and clear screen policy | | | |
| A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. | **Describe how** it was observed that a clear desk policy exists and is followed on the premises. |  |  |

### A.12 Operations security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **12.1 Operational procedures and responsibilities** | | | |
| **12.1.1** Documented operating procedures | | | |
| Operating procedures should be documented and made available to all users who need them. | **Identify** **all** operating procedure documents. |  |  |
| **12.1.2** Change management | | | |
| Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  |  |
| **12.1.3** Capacity management | | | |
| The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. | **Identifiy** how resources are monitored. |  |  |
| **12.1.4** Separation of development, testing and operational environments | | | |
| Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. | **Identify the network documentation** that illustrates that the development/test environments are separate from the production environment(s). |  |  |
| **Describe how** network device configurations were examined to verify that the development/test environments are separate from the production environment(s). |  |
| **12.2 Protection from malware** | | | |
| **12.2.1** Controls against malware | | | |
| Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. | **Identify** **the vendor documentation** reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| * Detect all known types of malicious software, |  |
| * Remove all known types of malicious software, and |  |
| * Protect against all known types of malicious software. |  |
| **12.3 Backup** | | | |
| **12.3.1** Information backup | | | |
| Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. | **Identify** **the assessor who attests b**ackup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy. |  |  |
| **12.4 Logging and monitoring** | | | |
| **12.4.1** Event logging | | | |
| Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. | **Identify the responsible personnel** interviewed who confirm the following from 10.2.1-10.2.7 are logged:   * All individual access to confidential data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |  |
| **Identify the sample of audit logs** observed to verify the following from 10.2.1-10.2.7 are logged:   * All individual access to confidential data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including.   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |
| **12.4.2** Protection of log information | | | |
| Logging facilities and log information should be protected against tampering and unauthorized access. | **Describe how** system configurations and permissions were examined to verify that current audit trail files are protected from unauthorized modifications. (e.g., via access control mechanisms, physical segregation, and/or network segregation). |  |  |
| **12.4.3** Administrator and operator logs | | | |
| System administrator and system operator activities should be logged and the logs protected and regularly reviewed. | **Describe how** configuration settings were observed to verify all actions taken by any individual with root or administrative privileges are logged. |  |  |
| **12.4.4** Clock synchronization | | | |
| The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source. | **Identify** **the documented process for acquiring, distributing, and storing the correct time within the organization** examined to verify that the process defines the following:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. * Systems receive time information only from designated central time server(s). |  |  |
| **12.5 Control of operational software** | | | |
| **12.5.1** Installation of software on operational systems | | | |
| Procedures should be implemented to control the installation of software on operational systems. | **Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. |  |  |
| **12.6 Technical Vulnerability Management** | | | |
| **12.6.1** Management of technical vulnerabilities | | | |
| Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. | **Identify** **the documented policies and procedures** related to security-patch installation examined to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame. |  |  |
| **12.6.2** Restrictions on software installation | | | |
| Rules governing the installation of software by users should be established and implemented. | **Identify** **the assessor who attests** rules governing the installation of software by users should be established and implemented. |  |  |
| **12.7 Information systems audit considerations** | | | |
| **12.7.1** Information systems audit controls | | | |
| Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes. | **Identify** **the assessor who attests** audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimize disruptions to business processes. |  |  |

### A.13 Communications security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **13.1 Network security management** | | | |
| **13.1.1** Network controls | | | |
| Networks should be managed and controlled to protect information in systems and applications. | **Identify the document(s)** reviewed to verify procedures define the formal processes for: | |  |
| * Testing and approval of all network connections. |  |
| * Testing and approval of all changes to firewall and router configurations. |  |
| **13.1.2** Security of network services | | | |
| Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced. | **Identify** **the assessor who attests** Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced. |  |  |
| **13.1.3** Segregation in networks | | | |
| Groups of information services, users and information systems should be segregated on networks. | **Identify** **the assessor who attests** Groups of information services, users and information systems are segregated on networks. |  |  |
| **13.2 Information transfer** | | | |
| **13.2.1** Information transfer policies and procedures | | | |
| Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. | **Identify the document** reviewed to verify that processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. |  |  |
| **13.2.2** Agreements on information transfer | | | |
| Agreements should address the secure transfer of business information between the organization and external parties. | **Identify** **the assessor who attests a**greements address the secure transfer of business information between the organization and external parties. |  |  |
| **13.2.3** Electronic messaging | | | |
| Information involved in electronic messaging should be appropriately protected. | **Indicate** **whether** end-user messaging technologies are used to send confidential data. **(yes/no)** |  |  |
| *If “no,” mark the remainder of 4.2.a as “Not Applicable” and proceed to 4.2.b.*  *If “yes,” complete the following:* | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **Describe how** the sample of outbound transmissions observed as they occurred to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **13.2.4** Confidentiality or non-disclosure agreements | | | |
| Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, regularly reviewed and documented. | **Identify** **the assessor who attests** requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information are identified, regularly reviewed and documented. |  |  |

### A.14 System acquisition, development and maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **14.1 Security requirements of information systems** | | | |
| **14.1.1** Information security requirements analysis and specification | | | |
| The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems. | **Identify** **the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network |  |  |
| **Identify** **the personnel** interviewed for this testing procedure. |  |
| For the interview, **summarize the relevant details** discussed that verify: | |
| * System configuration standards are applied when new systems are configured |  |
| * System configuration standards are verified as being in place before a system is installed on the network. |  |
| **14.1.2** Securing application services on public networks | | | |
| Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. | **Describe** **the sample** of inbound and outbound transmissions observed as they occurred. |  |  |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all confidential data is encrypted with strong cryptography during transit. |  |
| **14.1.3** Protecting application services transactions | | | |
| Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. | **Identify** **the assessor who attests** users are trained and applications require secure connections to communicate. |  |  |
| **14.2 Security in development and support processes** | | | |
| **14.2.1** Secure development policy | | | |
| Rules for the development of software and systems should be established and applied to developments within the organization. | **Identify** **the assessor who attests** development systems and software follow best practice for security within the organization. |  |  |
| **14.2.2** System change control procedures | | | |
| Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  |  |
| **14.2.3** Technical review of applications after operating platform changes | | | |
| When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | **Identify** **the assessor who attests** when operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.evelopment systems and software follow best practice for security within the organization. |  |  |
| **14.2.4** Restrictions on changes to software packages | | | |
| Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled. | **Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  |  |
| **Identify the personnel assigned to production environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  |
| **Describe how** processes were observed to verify that separation of duties is in place between development/test environments and the production environment. |  |
| **14.2.5** Secure system engineering principles | | | |
| Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts. | **Identify** **the document** that defines software development processes based on industry standards and/or best practices. |  |  |
| **Identify** the industry standards and/or best practices used. |  |
| **14.2.6** Secure development environment | | | |
| Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. | **Identify** **the assessor who attests** development systems and software follow best practice for security within the organization. |  |  |
| **14.2.7** Outsourced development | | | |
| The organization should supervise and monitor the activity of outsourced system development. | **Identify** **the document** that describes how the organization should supervise and monitor the activity of outsourced system development. |  |  |
| **14.2.8** System security testing | | | |
| Testing of security functionality should be carried out during development. | **Identify** **the document** that describes how testing of security functionality should be carried out during development. |  |  |
| **14.2.9** System acceptance testing | | | |
| Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. | **Identify** **the document** that describes User Acceptance testing |  |  |
| **14.3 Test data** | | | |
| **14.3.1** Protection of test data | | | |
| Test data should be selected carefully, protected and controlled. | **Identify** **the document** that describes how test data is protected. |  |  |

### A.15 Supplier relationships

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **15.1 Information security in supplier relationships** | | | |
| **15.1.1** Information security policy for supplier relationships | | | |
| Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets should be agreed with the supplier and documented. | **Identify** **the document** that contains Information security policy for supplier relationships. |  |  |
| **15.1.2** Addressing security within supplier agreements | | | |
| All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization’s information. | **Identify** **the document** addressing security within supplier agreements. |  |  |
| **15.1.3** Information and communication technology supply chain | | | |
| Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain. | **Identify** **the document** that addresses Information and communication technology supply chain |  |  |
| **15.2 Supplier service delivery management** | | | |
| **15.2.1** Monitoring and review of supplier services | | | |
| Organizations should regularly monitor, review and audit supplier service delivery. | **Describe how** it was verified that the procedures for proper due diligence prior to engaging a service provider are implemented, as documented in the policies and procedures. |  |  |
| **15.2.2** Managing changes to supplier services | | | |
| Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. | **Identify** **the assessor who attests** when changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. |  |  |

### A.16 Information security incident management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **16.1 Management of information security incidents and improvements** | | | |
| **16.1.1** Responsibilities and procedures | | | |
| Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. |  |  |
| **16.1.2** Reporting information security events | | | |
| Information security events should be reported through appropriate management channels as quickly as possible. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Communication strategies. |  |  |
| **16.1.3** Reporting information security weaknesses | | | |
| Employees and contractors using the organization’s information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Reporting information security weaknesses |  |  |
| **16.1.4** Assessment of and decision on information security events | | | |
| Information security events should be assessed and it should be decided if they are to be classified as information security incidents. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Assessment of and decision on information security events. |  |  |
| **16.1.5** Response to information security incidents | | | |
| Information security incidents should be responded to in accordance with the documented procedures. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Business recovery and continuity procedures. * Analysis of legal requirements for reporting compromises. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  |  |
| **16.1.6** Learning from information security incidents | | | |
| Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **16.1.7** Collection of evidence | | | |
| The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Collection of evidence |  |  |

### A.17 Information security aspects of business continuity management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **17.1 Information security continuity** | | | |
| **17.1.1** Planning information security continuity | | | |
| The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show** Planning information security continuity |  |  |
| **17.1.2** Implementing information security continuity | | | |
| The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show I**mplementing information security continuity |  |  |
| **17.1.3** Verify, review and evaluate information security continuity | | | |
| The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show it** verifies, review and evaluate information security continuity |  |  |
| **17.2 Redundancies** | | | |
| **17.2.1** Availability of information processing facilities | | | |
| Information processing facilities should be implemented with redundancy sufficient to meet availability requirements. | **Identify** **all locations** where backup media is stored. |  |  |
| **Describe how** it was observed that backup media storage is stored in a secure location. |  |

### A.18 Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **18.1 Compliance with legal and contractual requirements** | | | |
| **18.1.1** Identification of applicable legislation and contractual requirements | | | |
| All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization. | **Identify the documented** policy that contains applicable legislation and contractual requirements. |  |  |
| **18.1.2** Intellectual property rights | | | |
| Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. | **Identify the documented** policy that contains intellectual property rights. |  |  |
| **18.1.3** Protection of records | | | |
| Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislated, regulatory, contractual and business requirements. | **Identify the documented** policy that contains protection of records. |  |  |
| **18.1.4** Privacy and protection of personally identifiable information | | | |
| Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable. | **Identify the documented** policy that contains the privacy and protection of personally identifiable information. |  |  |
| **18.1.5** Regulation of cryptographic controls | | | |
| Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations. | **Identify the documented** policy that contains the regulation of cryptographic controls. |  |  |
| **18.2 Information security reviews** | | | |
| **18.2.1** Independent review of information security | | | |
| The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. | **Identify the documented** audits that have occurred. |  |  |
| **18.2.2** Compliance with security policies and standards | | | |
| Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. | **Identify the document** reviewed to verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. |  |  |
| **Describe how** the information security policy was verified to be: | |
| * Reviewed at least annually. |  |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  |
| **18.2.3** Technical compliance review | | | |
| Information systems should be regularly reviewed for compliance with the organization’s information security policies and standards. | **Identify** **the policy documentation** verified to define that system configuration standards are updated as new vulnerability issues are identified |  |  |
| **Identify** **the personnel** interviewed for this testing procedure. |  |
| For the interview, **summarize the relevant details** discussed that verify that the process is implemented. |  |

## ISO 27002

### A.5 Information Security Policies

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **5.1 Management Direction for Information Security** | | | |
| **5.1.1** Information security policy document. | | | |
| An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **5.1.2** Review of the policies for information security. | | | |
| The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | **Identify** **the information security policies and procedures** reviewed to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: |  |  |

### A.6 Organization of Information Security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **6.1 Internal organization** | | | |
| **6.1.1** Information security roles and responsibilities | | | |
| All information security responsibilities should be defined and allocated. | **Identify** **the information security policies and procedures** reviewed to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: |  |  |
| **6.1.2** Segregation of duties | | | |
| Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. | **Identify the documented policy** reviewed to verify responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. |  |  |
| **6.1.3** Contact with authorities | | | |
| Appropriate contacts with relevant authorities should be maintained. | **Identify the documented policy** reviewed to verify appropriate contacts with relevant authorities should be maintained. |  |  |
| **6.1.4** Contact with special interest groups | | | |
| Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. | **Identify the documented policy** reviewed to verify appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. |  |  |
| **6.1.5** Information security in project management | | | |
| Information security should be addressed in project management, regardless of the type of the project. | **Identify** the personnel interviewed to confirm that Information Security is addressed in project management. |  |  |
| **6.2**  **Mobile devices and teleworking** | | | |
| **6.2.1** Mobile device policy | | | |
| A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices. | **Indicate whether** mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network are used to access the organization’s network. **(yes/no)** |  |  |
| *If “no,”* **identify** **the document** reviewed that explicitly prohibits mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network from being used to access the organization’s network. |  |
| *If “yes,”* **identify** **the documented policies and configuration standards** that define the following:   * Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network, and which are also used to access the network. * Specific configuration settings are defined for personal firewall software. * Personal firewall software is configured to actively run. * Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. |  |
| **6.2.2** Teleworking | | | |
| A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. | **Identify the documented policy** reviewed to verify policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. |  |  |

### A.7 Human resources security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **7.1 Prior to employment** | | | |
| **7.1.1** Screening | | | |
| Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | **Identify the Human Resources personnel** interviewed who confirm background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  |  |
| **Describe how** it was observed that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  |
| **7.1.2** Terms and conditions of employment | | | |
| The contractual agreements with employees and contractors should state their and the organization’s responsibilities for information security. | **Describe how** it was verified that, per the security awareness program, all personnel: | |  |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  |
| * Provide an acknowledgement at least annually. |  |
| **7.2 During employment** | | | |
| **7.2.1** Management responsibilities | | | |
| Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. | **Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **7.2.2** Information security awareness, education and training | | | |
| All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. | **Provide the name of the assessor** who attests that the security awareness program was verified to provide awareness to all personnel about the cardholder data security policy and procedures. |  |  |
| **Identify the documented security awareness program procedures and additional documentation** examined to verify that:   * The security awareness program provides multiple methods of communicating awareness and educating personnel. * Personnel attend security awareness training: * Upon hire, and * At least annually * Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. |  |
| **7.2.3** Disciplinary process | | | |
| There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. | **Identify the documented policy** reviewed to verify appropriate contacts with relevant authorities should be maintained. |  |  |
| **7.3 Termination and change of employment** | | | |
| **7.3.1** Termination or change of employment responsibilities | | | |
| Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. | **Identify the documented policy** reviewed to verify responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. |  |  |

### A.8 Asset management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **8.1 Responsibility for assets** | | | |
| **8.1.1** Inventory of assets | | | |
| Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. | **Describe how** the system inventory was examined to verify that a list of hardware and software components is: | |  |
| * Maintained |  |
| * Includes a description of function/use for each |  |
| **8.1.2** Ownership of assets | | | |
| Assets maintained in the inventory should be owned. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.1.3** Acceptable use of assets | | | |
| Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  |  |
| **8.1.4** Return of assets | | | |
| All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.2 Information classification** | | | |
| **8.2.1** Classification of information | | | |
| Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. | **Identify the documented policy** reviewed to verify Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. |  |  |
| **8.2.2** Labelling of information | | | |
| An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization. | **Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine:   * Owner * Contact Information * Purpose |  |  |
| **8.2.3** Handling of assets | | | |
| Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.3 Media handling** | | | |
| **8.3.1** Management of removable media | | | |
| Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. | **Describe how** media was observed to be classified so the sensitivity of the data can be determined. |  |  |
| **8.3.2** Disposal of media | | | |
| Media should be disposed of securely when no longer required, using formal procedures. | **Identify** **the responsible personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  |  |
| **Provide the name of the assessor** who attests that the procedures state that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. |  |
| **8.3.3** Physical media transfer | | | |
| Media containing information should be protected against unauthorized access, misuse or corruption during transportation. | **Identify** **responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |  |
| **Describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |

### A.9 Access Control

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **9.1 Business requirements of access control** | | | |
| **9.1.1** Access control policy | | | |
| An access control policy should be established, documented and reviewed based on business and information security requirements. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.1.2** Access to networks and network services | | | |
| Users should only be provided with access to the network and network services that they have been specifically authorized to use. | **Identify the sample** of user IDs examined for this testing procedure. |  |  |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | |
| * Documented approval exists for the assigned privileges. |  |
| * The approval was by authorized parties. |  |
| * That specified privileges match the roles assigned to the individual. |  |
| **9.2 User access management** | | | |
| **9.2.1** User registration and de-registration | | | |
| A formal user registration and de-registration process should be implemented to enable assignment of access rights. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.2.2** User access provisioning | | | |
| A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services. | **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **9.2.3** Management of privileged access rights | | | |
| The allocation and use of privileged access rights should be restricted and controlled. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.2.4** Management of secret authentication information for users | | | |
| The allocation of secret authentication information should be controlled through a formal management process. | **Identify** **the document** that contains the management of secret authentication information for users. |  |  |
| **9.2.5** Review of user access rights | | | |
| Asset owners should review users’ access rights at regular intervals. | **Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled. |  |  |
| **9.2.6** Removal or adjustment of user access rights | | | |
| The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. | **Identify** **the sample** of users terminated in the past six months that were selected for this testing procedure. |  |  |
| **Describe how** the current user access lists for ***local access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **9.3 User responsibilities** | | | |
| **9.3.1** User of secret authentication information | | | |
| Users should be required to follow the organization’s practices in the use of secret authentication information. | **Identify** **the document** that contains the management of secret authentication information for users. |  |  |
| **9.4 System and application access control** | | | |
| **9.4.1** Information access restriction | | | |
| Access to information and application system functions should be restricted in accordance with the access control policy. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates:   * Access to information and application system. |  |  |
| **9.4.2** Secure log-on procedures | | | |
| Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure. | **Identify** all databases containing cardholder data. |  |  |
| **Describe how** database and/or application configuration settings verified that all users are authenticated prior to access. |  |
| **9.4.3** Password management system | | | |
| Password management systems should be interactive and should ensure quality passwords. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or cardholder data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |
| **9.4.4** Use of privileged utility programs | | | |
| The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | **Identify the assessor** who attests that users cannot installed software or utility programs and that they are tightly controlled. |  |  |
| **9.4.5** Access control to program source code | | | |
| Access to program source code should be restricted. | **Identify the assessor** who attests that access to program source code is restricted. |  |  |

### A.10 Cryptography

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **10.1 Cryptographic controls** | | | |
| **10.1.1** Policy on the use of cryptographic controls | | | |
| A policy on the use of cryptographic controls for protection of information should be developed and implemented. | **Identify** **the documentation** examined to verify that the NPI is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  |  |
| **10.1.2** Key management | | | |
| A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle. | **Identify** **the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. |  |  |

### A.11 Physical and environmental security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **11.1 Secure areas** | | | |
| **11.1.1** Physical security perimeter | | | |
| Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. | **Identify and briefly describe** all of the following with systems in the confidential data environment: | |  |
| * All computer rooms |  |
| * All data centers |  |
| * Any other physical areas |  |
| *For each area identified (add rows as needed),* complete the following: | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **Identify** the randomly selected systems in the confidential environment for which a system administrator login attempt was observed. |  |
| **Describe how** consoles for the randomly selected systems were observed to verify that they are “locked” when not in use to prevent unauthorized use. |  |
| **11.1.2** Physical entry controls | | | |
| Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. | **Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access. |  |  |
| **11.1.3** Securing offices, rooms, facilities | | | |
| Physical security for offices, rooms and facilities should be designed and applied. | **Describe** either the video cameras or access control mechanisms (or both) observed to monitor the entry/exit points to sensitive areas. |  |  |
| **11.1.4** Protecting against external and environmental threats | | | |
| Physical protection against natural disasters, malicious attack or accidents should be designed and applied. | **Identify the documented**  **Business Continuity and Disaster Recovery Policy to show** Protecting against external and environmental threats |  |  |
| **11.1.5** Working in secure areas | | | |
| Procedures for working in secure areas should be designed and applied. | **Identify** **the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  |  |
| **11.1.6** Delivery and loading areas | | | |
| Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. | **Describe** how access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. |  |  |
| **11.2 Equipment** | | | |
| **11.2.1** Equipment siting and protection | | | |
| Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. | **Identify** **the assessor who confirms** equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |  |  |
| **11.2.2** Supporting utilities | | | |
| Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. | **Identify** **the assessor who confirms** equipment is protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |
| **11.2.3** Cabling security | | | |
| Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage. | **Identify** **the assessor who confirms** power and telecommunications cabling carrying data or supporting information services is protected from interception, interference or damage. |  |  |
| **11.2.4** Equipment maintenance | | | |
| Equipment should be correctly maintained to ensure its continued availability and integrity. | **Identify** **the assessor who confirms** equipment is correctly maintained to ensure its continued availability and integrity. |  |  |
| **11.2.5** Removal of assets | | | |
| Equipment, information or software should not be taken off-site without prior authorization. | **Identify** **the assessor who confirms** equipment, information or software is not taken off-site without prior authorization. |  |  |
| **11.2.6** Security of equipment and assets off-premises | | | |
| Security should be applied to off-site assets taking into account the different risks of working outside the organization’s. premises | **Identify** **the assessor who confirms** security is applied to off-site assets taking into account the different risks of working outside the organization’s premises. |  |  |
| **11.2.7** Secure disposal or re-use of equipment | | | |
| All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. | **Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Confidential data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). |  |  |
| **11.2.8** Unattended user equipment | | | |
| Users should ensure that unattended equipment has appropriate protection. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  |  |
| **11.2.9** Clear desk and clear screen policy | | | |
| A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. | **Describe how** it was observed that a clear desk policy exists and is followed on the premises. |  |  |

### A.12 Operations security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **12.1 Operational procedures and responsibilities** | | | |
| **12.1.1** Documented operating procedures | | | |
| Operating procedures should be documented and made available to all users who need them. | **Identify** **all** operating procedure documents. |  |  |
| **12.1.2** Change management | | | |
| Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  |  |
| **12.1.3** Capacity management | | | |
| The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. | **Identifiy** how resources are monitored. |  |  |
| **12.1.4** Separation of development, testing and operational environments | | | |
| Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. | **Identify the network documentation** that illustrates that the development/test environments are separate from the production environment(s). |  |  |
| **Describe how** network device configurations were examined to verify that the development/test environments are separate from the production environment(s). |  |
| **12.2 Protection from malware** | | | |
| **12.2.1** Controls against malware | | | |
| Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. | **Identify** **the vendor documentation** reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| * Detect all known types of malicious software, |  |
| * Remove all known types of malicious software, and |  |
| * Protect against all known types of malicious software. |  |
| **12.3 Backup** | | | |
| **12.3.1** Information backup | | | |
| Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. | **Identify** **the assessor who attests b**ackup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy. |  |  |
| **12.4 Logging and monitoring** | | | |
| **12.4.1** Event logging | | | |
| Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. | **Identify the responsible personnel** interviewed who confirm the following are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |  |
| **Identify the sample of audit logs** selected for reviewing all the above is logged. |  |
| **12.4.2** Protection of log information | | | |
| Logging facilities and log information should be protected against tampering and unauthorized access. | **Describe how** system configurations and permissions were examined to verify that current audit trail files are protected from unauthorized modifications. (e.g., via access control mechanisms, physical segregation, and/or network segregation). |  |  |
| **12.4.3** Administrator and operator logs | | | |
| System administrator and system operator activities should be logged and the logs protected and regularly reviewed. | **Describe how** configuration settings were observed to verify all actions taken by any individual with root or administrative privileges are logged. |  |  |
| **12.4.4** Clock synchronization | | | |
| The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source. | **Identify** **the documented time-synchronization configuration standards** examined to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. |  |  |
| **12.5 Control of operational software** | | | |
| **12.5.1** Installation of software on operational systems | | | |
| Procedures should be implemented to control the installation of software on operational systems. | **Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. |  |  |
| **12.6 Technical Vulnerability Management** | | | |
| **12.6.1** Management of technical vulnerabilities | | | |
| Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. | **Identify** **the documented policies and procedures** related to security-patch installation examined to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame. |  |  |
| **12.6.2** Restrictions on software installation | | | |
| Rules governing the installation of software by users should be established and implemented. | **Identify** **the assessor who attests** rules governing the installation of software by users should be established and implemented. |  |  |
| **12.7 Information systems audit considerations** | | | |
| **12.7.1** Information systems audit controls | | | |
| Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes. | **Identify** **the assessor who attests** audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimize disruptions to business processes. |  |  |

### A.13 Communications security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **13.1 Network security management** | | | |
| **13.1.1** Network controls | | | |
| Networks should be managed and controlled to protect information in systems and applications. | **Identify the document(s)** reviewed to verify procedures define the formal processes for: | |  |
| * Testing and approval of all network connections. |  |
| * Testing and approval of all changes to firewall and router configurations. |  |
| **13.1.2** Security of network services | | | |
| Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced. | **Identify** **the assessor who attests** Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced. |  |  |
| **13.1.3** Segregation in networks | | | |
| Groups of information services, users and information systems should be segregated on networks. | **Identify** **the assessor who attests** Groups of information services, users and information systems are segregated on networks. |  |  |
| **13.2 Information transfer** | | | |
| **13.2.1** Information transfer policies and procedures | | | |
| Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. | **Identify the document** reviewed to verify that processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. |  |  |
| **13.2.2** Agreements on information transfer | | | |
| Agreements should address the secure transfer of business information between the organization and external parties. | **Identify** **the assessor who attests a**greements address the secure transfer of business information between the organization and external parties. |  |  |
| **13.2.3** Electronic messaging | | | |
| Information involved in electronic messaging should be appropriately protected. | **Indicate** **whether** end-user messaging technologies are used to send cardholder data. **(yes/no)** |  |  |
| *If “no,” mark the remainder of 4.2.a as “Not Applicable” and proceed to 4.2.b.*  *If “yes,” complete the following:* | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **Describe** **the sample** of outbound transmissions that were observed as they occurred. |  |
| **Describe how** the sample of outbound transmissions verified that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **13.2.4** Confidentiality or non-disclosure agreements | | | |
| Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, regularly reviewed and documented. | **Identify** **the assessor who attests** requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information are identified, regularly reviewed and documented. |  |  |

### A.14 System acquisition, development and maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **14.1 Security requirements of information systems** | | | |
| **14.1.1** Information security requirements analysis and specification | | | |
| The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems. | **Identify** **the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network |  |  |
| **Identify** **the responsible personnel** interviewed who confirm that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. |  |
| **14.1.2** Securing application services on public networks | | | |
| Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. | **Describe** **the sample** of inbound and outbound transmissions observed as they occurred. |  |  |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all confidential data is encrypted with strong cryptography during transit. |  |
| **14.1.3** Protecting application services transactions | | | |
| Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. | **Identify** **the assessor who attests** users are trained and applications require secure connections to communicate. |  |  |
| **14.2 Security in development and support processes** | | | |
| **14.2.1** Secure development policy | | | |
| Rules for the development of software and systems should be established and applied to developments within the organization. | **Identify** **the assessor who attests** development systems and software follow best practice for security within the organization. |  |  |
| **14.2.2** System change control procedures | | | |
| Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  |  |
| **14.2.3** Technical review of applications after operating platform changes | | | |
| When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | **Identify** **the responsible personnel** interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  |  |
| **14.2.4** Restrictions on changes to software packages | | | |
| Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled. | **Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  |  |
| **Identify the personnel assigned to production environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  |
| **Describe how** processes were observed to verify that separation of duties is in place between development/test environments and the production environment. |  |
| **14.2.5** Secure system engineering principles | | | |
| Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts. | **Identify** **the document** examined to verify that software-development processes are based on industry standards and/or best practices. |  |  |
| **14.2.6** Secure development environment | | | |
| Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. | **Identify** **the assessor who attests** development systems and software follow best practice for security within the organization. |  |  |
| **14.2.7** Outsourced development | | | |
| The organization should supervise and monitor the activity of outsourced system development. | **Identify** **the document** that describes how the organization should supervise and monitor the activity of outsourced system development. |  |  |
| **14.2.8** System security testing | | | |
| Testing of security functionality should be carried out during development. | **Identify** **the document** that describes how testing of security functionality should be carried out during development. |  |  |
| **14.2.9** System acceptance testing | | | |
| Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. | **Identify** **the document** that describes User Acceptance testing |  |  |
| **14.3 Test data** | | | |
| **14.3.1** Protection of test data | | | |
| Test data should be selected carefully, protected and controlled. | **Identify** **the document** that describes how test data is protected. |  |  |

### A.15 Supplier relationships

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **15.1 Information security in supplier relationships** | | | |
| **15.1.1** Information security policy for supplier relationships | | | |
| Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets should be agreed with the supplier and documented. | **Identify** **the document** that contains Information security policy for supplier relationships. |  |  |
| **15.1.2** Addressing security within supplier agreements | | | |
| All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization’s information. | **Identify** **the document** addressing security within supplier agreements. |  |  |
| **15.1.3** Information and communication technology supply chain | | | |
| Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain. | **Identify** **the document** that addresses Information and communication technology supply chain |  |  |
| **15.2 Supplier service delivery management** | | | |
| **15.2.1** Monitoring and review of supplier services | | | |
| Organizations should regularly monitor, review and audit supplier service delivery. | **Identify the documented policies and procedures** reviewed to verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data. |  |  |
| **15.2.2** Managing changes to supplier services | | | |
| Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. | **Identify** **the assessor who attests** when changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. |  |  |

### A.16 Information security incident management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **16.1 Management of information security incidents and improvements** | | | |
| **16.1.1** Responsibilities and procedures | | | |
| Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. |  |  |
| **16.1.2** Reporting information security events | | | |
| Information security events should be reported through appropriate management channels as quickly as possible. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Communication strategies. |  |  |
| **16.1.3** Reporting information security weaknesses | | | |
| Employees and contractors using the organization’s information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Reporting information security weaknesses |  |  |
| **16.1.4** Assessment of and decision on information security events | | | |
| Information security events should be assessed and it should be decided if they are to be classified as information security incidents. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Assessment of and decision on information security events. |  |  |
| **16.1.5** Response to information security incidents | | | |
| Information security incidents should be responded to in accordance with the documented procedures. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Business recovery and continuity procedures. * Analysis of legal requirements for reporting compromises. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  |  |
| **16.1.6** Learning from information security incidents | | | |
| Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **16.1.7** Collection of evidence | | | |
| The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Collection of evidence |  |  |

### A.17 Information security aspects of business continuity management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **17.1 Information security continuity** | | | |
| **17.1.1** Planning information security continuity | | | |
| The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show** Planning information security continuity |  |  |
| **17.1.2** Implementing information security continuity | | | |
| The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show I**mplementing information security continuity |  |  |
| **17.1.3** Verify, review and evaluate information security continuity | | | |
| The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show it** verifies, review and evaluate information security continuity |  |  |
| **17.2 Redundancies** | | | |
| **17.2.1** Availability of information processing facilities | | | |
| Information processing facilities should be implemented with redundancy sufficient to meet availability requirements. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  |  |

### A.18 Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **18.1 Compliance with legal and contractual requirements** | | | |
| **18.1.1** Identification of applicable legislation and contractual requirements | | | |
| All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization. | **Identify the documented** policy that contains applicable legislation and contractual requirements. |  |  |
| **18.1.2** Intellectual property rights | | | |
| Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. | **Identify the documented** policy that contains intellectual property rights. |  |  |
| **18.1.3** Protection of records | | | |
| Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislated, regulatory, contractual and business requirements. | **Identify the documented** policy that contains protection of records. |  |  |
| **18.1.4** Privacy and protection of personally identifiable information | | | |
| Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable. | **Identify the documented** policy that contains the privacy and protection of personally identifiable information. |  |  |
| **18.1.5** Regulation of cryptographic controls | | | |
| Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations. | **Identify the documented** policy that contains the regulation of cryptographic controls. |  |  |
| **18.2 Information security reviews** | | | |
| **18.2.1** Independent review of information security | | | |
| The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. | **Identify the documented** audits that have occurred. |  |  |
| **18.2.2** Compliance with security policies and standards | | | |
| Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. | **Describe how** the information security policy was verified to be: | |  |
| * Reviewed at least annually. |  |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  |
| **18.2.3** Technical compliance review | | | |
| Information systems should be regularly reviewed for compliance with the organization’s information security policies and standards. | **Identify** **the policy documentation** examined toverify thatsystem configuration standards are updated as new vulnerability issues are identified. |  |  |
| **Identify** **the responsible personnel** interviewed who confirm thatsystem configuration standards are updated as new vulnerability issues are identified. |  |

## Mass 201 CMR 17.00

|  |  |  |  |
| --- | --- | --- | --- |
| Section | Control Description | Control Effectiveness | Notes |
| 17.03: Duty to Protect and Standards for Protecting Personal Information | | | |
| 17.03(1) | Develop, implement, maintain, and monitor a comprehensive, written information security program applicable to any records containing personal information. Such comprehensive information security program must be reasonably consistent with industry standards, and must contain administrative, technical, and physical safeguards to ensure the security and confidentiality of personal information. |  |  |
| 17.03(3)(a) | Designate one or more employees to maintain the comprehensive information security program. |  |  |
| 17.03(3)(b) | Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:   1. ongoing employee (including temporary and contract employee) training; 2. employee compliance with policies and procedures; and 3. means for detecting and preventing security system failures. |  |  |
| 17.03(3)(c) | Develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises. |  |  |
| 17.03(3)(d) | Impose disciplinary measures for violations of the comprehensive information security program rules. |  |  |
| 17.03(3)(e) | Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names. |  |  |
| 17.03(3)(f) | Take all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00. |  |  |
| 17.03(3)(g) | Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limit the time such information is retained to that reasonably necessary to accomplish such purpose; and limit access to those persons who are reasonable required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements. |  |  |
| 17.03(3)(h) | Identify paper, electronic and other records, computer systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information. |  |  |
| 17.03(3)(i) | Reasonably restrict physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and store such records and data in locked facilities, storage area or containers. |  |  |
| 17.03(3)(j) | Regularly monitor to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrade information safeguards as necessary to limit risks. |  |  |
| 17.03(3)(k) | Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information. |  |  |
| 17.03(3)(l) | Document responsive actions taken in connection with any incident involving a breach of security, and perform a post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information. |  |  |
| 17.04: Computer System Security Requirements | | | |
| 17.04(1) | Secure user authentication protocols including:  (a) control of user IDs and other identifiers;  (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;  (c) control of data security passwords to ensure that such passwords are kept in a safe location and/or format that does not compromise the security of the data they protect;  (d) restrict access to active users and active user accounts only;  (e) block access to user identification after multiple unsuccessful attempts to gain access or the limitation places on access for the particular system. |  |  |
| 17.04(2)(a) | Restrict access to records and files containing personal information to those who need such information to perform their job duties. |  |  |
| 17.04(2)(b) | Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls. |  |  |
| 17.04(3) | To the extent technically feasible, encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all data containing personal information to be transmitted wirelessly. |  |  |
| 17.04(4) | Reasonably monitor systems, for unauthorized user of or access to personal information. |  |  |
| 17.04(5) | Encrypt all personal information stored on laptops or other portable devices. |  |  |
| 17.04(6) | For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information. |  |  |
| 17.04(7) | Implement reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis. |  |  |
| 17.04(8) | Educate and train all employees on the proper use of the computer security system and the importance of personal information security. |  |  |

## Mass 201 CMR 17.00

|  |  |  |  |
| --- | --- | --- | --- |
| **Mass 201 CMR 17.00 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **17.03: Duty to Protect and Standards for Protecting Personal Information** | | | | |
| **17.03(1)** | | | | |
| Develop, implement, maintain, and monitor a comprehensive, written information security program applicable to any records containing personal information. Such comprehensive information security program must be reasonably consistent with industry standards, and must contain administrative, technical, and physical safeguards to ensure the security and confidentiality of personal information. | **Identify the documented information security policy** examined. |  |  | |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |  | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **17.03(3)(a)** | | | | |
| Designate one or more employees to maintain the comprehensive information security program. | **Identify the personnel** designated to maintain the comprehensive information security program. |  |  | |
| **17.03(3)(b)** | | | | |
| Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:   1. ongoing employee (including temporary and contract employee) training; 2. employee compliance with policies and procedures; and   means for detecting and preventing security system failures. | **Describe how** it was verified that an annual risk-assessment process is documented that: | |  | |
| * Identifies critical assets, threats and vulnerabilities. |  |
| * Results in formal, documented analysis of risk. |  |
| **17.03(3)(c)** | | | | |
| Develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises. | **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  |  | |
| **Describe how** media distribution is controlled, including distribution to individuals. |  |
| **17.03(3)(d)** | | | | |
| Impose disciplinary measures for violations of the comprehensive information security program rules. | **Identify the policies** and procedures that Impose disciplinary measures for violations of the comprehensive information security program rules. |  |  | |
| **17.03(3)(e)** | | | | |
| Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names. | **Identify** **the sample** of users terminated in the past six months selected. |  |  | |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **17.03(3)(f)** | | | | |
| Take all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00. | **Identify the documented policies and procedures to manage service providers with whom confidential data is shared, or that could affect the security of confidential data**, reviewed to verify policy defines the following:   * Maintain a list of service providers. * Maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s confidential data or sensitive authentication data, or manages the customer's confidential data environment on behalf of a customer. * Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. * Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. * Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  |  | |
| **17.03(3)(g)** | | | | |
| Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limit the time such information is retained to that reasonably necessary to accomplish such purpose; and limit access to those persons who are reasonable required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements. | **Identify the document** that gives procedures on limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected |  |  | |
| **17.03(3)(h)** | | | | |
| Identify paper, electronic and other records, computer systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information. | **Identify** **the data-flow diagram**(s) examined. |  |  | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  |
| For the interview, **summarize the relevant details discussed** to verify the diagram: | |
| * Shows all confidential data flows across systems and networks. |  |
| * Is kept current and updated as needed upon changes to the environment. |  |
| **17.03(3)(i)** | | | | |
| Reasonably restrict physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and store such records and data in locked facilities, storage area or containers. | **Identify the documented procedures for protecting confidential data** reviewed to verify controls for physically securing all media are defined. |  |  | |
| *For all types of media used,* **describe the controls** for physically securing the media used. |  |
| **17.03(3)(j)** | | | | |
| Regularly monitor to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrade information safeguards as necessary to limit risks. | **Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  |  | |
| **17.03(3)(k)** | | | | |
| Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information. | **Identify** any security measures reviewed or assessed internally or by an auditor. |  |  | |
| **17.03(3)(l)** | | | | |
| Document responsive actions taken in connection with any incident involving a breach of security, and perform a post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  | |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **17.04: Computer System Security Requirements** | | | | |
| **17.04(1)** | | | | |
| Secure user authentication protocols including:  (a) control of user IDs and other identifiers;  (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;  (c) control of data security passwords to ensure that such passwords are kept in a safe location and/or format that does not compromise the security of the data they protect;  (d) restrict access to active users and active user accounts only;  (e) block access to user identification after multiple unsuccessful attempts to gain access or the limitation places on access for the particular system. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or confidential data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  | |
| **17.04(2)(a)** | | | | |
| Restrict access to records and files containing personal information to those who need such information to perform their job duties. | **Identify** **the selected sample** of roles for this testing procedure. |  |  | |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **17.04(2)(b)** | | | | |
| Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls. | **Identify** **the responsible administrative personnel** interviewed for this testing procedure. |  |  | |
| For the interview, **summarize the relevant details discussed** to confirm that all users are assigned a unique ID for access to system components or confidential data. |  |
| **17.04(3)** | | | | |
| To the extent technically feasible, encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all data containing personal information to be transmitted wirelessly. | **Identify** all locations where confidential data is transmitted or received over open, public networks. |  |  | |
| **Identify** **the documented standards** examined. |  |
| **Describe how** the documented standards were examined and compared to system configurations to verify the use of: | |
| * Security protocols observed in use |  |
| * Strong cryptography for all locations |  |
| **17.04(4)** | | | | |
| Reasonably monitor systems, for unauthorized user of or access to personal information. | **Identify the responsible personnel** interviewed who confirm the following are logged:   * All individual access to confidential data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |  | |
| **Identify the sample of audit logs** observed to verify the following are logged:   * All individual access to confidential data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including.   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |
| **17.04(5)** | | | | |
| Encrypt all personal information stored on laptops or other portable devices. | **Indicate whether** disk encryption is used. **(yes/no)** |  |  | |
| *If “yes,” complete the remainder.*  *If “no,” mark the remainder as “Not Applicable.’* | |
| **Describe** the disk encryption mechanism(s) in use. |  |
| *For each disk encryption mechanism in use*, **describe how** the configuration was inspected and the authentication process observed to verify that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  |
| **17.04(6)** | | | | |
| For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information. | **Identify** **the documented policies and configuration standards** that define the following:   * Firewall software/hardware is required for all devices (containing personal information) that connect to the Internet when outside the network, and which are also used to access the network. |  |  | |
| **17.04(7)** | | | | |
| Implement reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are: | |  | |
| * Configured to perform automatic updates, and |  |
| * Configured to perform periodic scans. |  |
| **17.04(8)** | | | | |
| Educate and train all employees on the proper use of the computer security system and the importance of personal information security. | **Identify the documented security awareness program** reviewed to verify it provides awareness to all personnel about the importance of confidential data security. |  |  | |

## Mass 201 CMR 17.00

|  |  |  |  |
| --- | --- | --- | --- |
| **Mass 201 CMR 17.00 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **17.03: Duty to Protect and Standards for Protecting Personal Information** | | | |
| **17.03(1)** | | | |
| Develop, implement, maintain, and monitor a comprehensive, written information security program applicable to any records containing personal information. Such comprehensive information security program must be reasonably consistent with industry standards, and must contain administrative, technical, and physical safeguards to ensure the security and confidentiality of personal information. | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **17.03(3)(a)** | | | |
| Designate one or more employees to maintain the comprehensive information security program. | **Identify the personnel** designated to maintain the comprehensive information security program. |  |  |
| **17.03(3)(b)** | | | |
| Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:   1. ongoing employee (including temporary and contract employee) training; 2. employee compliance with policies and procedures; and   means for detecting and preventing security system failures. | **Provide the name of the assessor** who attests that the documented annual risk-assessment process:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. |  |  |
| **17.03(3)(c)** | | | |
| Develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises. | * **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  |  |
| **17.03(3)(d)** | | | |
| Impose disciplinary measures for violations of the comprehensive information security program rules. | **Identify the policies** and procedures that Impose disciplinary measures for violations of the comprehensive information security program rules. |  |  |
| **17.03(3)(e)** | | | |
| Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names. | **Identify** **the sample** of users terminated in the past six months selected. |  |  |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **17.03(3)(f)** | | | |
| Take all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00. | **Identify the documented policies and procedures to manage service providers with whom confidential data is shared, or that could affect the security of confidential data**, reviewed to verify policy defines the following:   * Maintain a list of service providers. * Maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s confidential data or sensitive authentication data, or manages the customer's confidential data environment on behalf of a customer. * Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. * Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. * Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  |  |
| **17.03(3)(g)** | | | |
| Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limit the time such information is retained to that reasonably necessary to accomplish such purpose; and limit access to those persons who are reasonable required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements. | **Identify the document** that gives procedures on limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected |  |  |
| **17.03(3)(h)** | | | |
| Identify paper, electronic and other records, computer systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information. | **Identify** **the data-flow diagram**(s) examined. |  |  |
| **Identify** **the responsible personnel** interviewed who confirm that the diagram:   * Shows all confidential data flows across systems and networks. * Is kept current and updated as needed upon changes to the environment. |  |
| **17.03(3)(i)** | | | |
| Reasonably restrict physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and store such records and data in locked facilities, storage area or containers. | * **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  |  |
| **17.03(3)(j)** | | | |
| Regularly monitor to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrade information safeguards as necessary to limit risks. | **Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  |  |
| **17.03(3)(k)** | | | |
| Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information. | **Identify** any security measures reviewed or assessed internally or by an auditor. |  |  |
| **17.03(3)(l)** | | | |
| Document responsive actions taken in connection with any incident involving a breach of security, and perform a post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **17.04: Computer System Security Requirements** | | | |
| **17.04(1)** | | | |
| Secure user authentication protocols including:  (a) control of user IDs and other identifiers;  (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;  (c) control of data security passwords to ensure that such passwords are kept in a safe location and/or format that does not compromise the security of the data they protect;  (d) restrict access to active users and active user accounts only;  (e) block access to user identification after multiple unsuccessful attempts to gain access or the limitation places on access for the particular system. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or confidential data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |
| **17.04(2)(a)** | | | |
| Restrict access to records and files containing personal information to those who need such information to perform their job duties. | **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **17.04(2)(b)** | | | |
| Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls. | * **Identify** **the responsible administrative personnel** interviewed who confirm that all users are assigned a unique ID for access to system components or confidential data. |  |  |
| **17.04(3)** | | | |
| To the extent technically feasible, encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all data containing personal information to be transmitted wirelessly. | **Identify** all locations where confidential data is transmitted or received over open, public networks. |  |  |
| **Identify** **the documented standards** examined. |  |
| **Describe how** the documented standards were examined and compared to system configurations to verify the use of: | |
| * Security protocols observed in use |  |
| * Strong cryptography for all locations |  |
| **17.04(4)** | | | |
| Reasonably monitor systems, for unauthorized user of or access to personal information. | **Identify the responsible personnel** interviewed who confirm the following are logged:   * All individual access to confidential data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |  |
| **Identify the sample of audit logs** observed to contain the information above. |  |
| **17.04(5)** | | | |
| Encrypt all personal information stored on laptops or other portable devices. | **Indicate whether** disk encryption is used. **(yes/no)** |  |  |
| *If “yes,” complete the remainder.*  *If “no,” mark the remainder as “Not Applicable.’* | |
| **Describe** the disk encryption mechanism(s) in use. |  |
| *For each disk encryption mechanism in use*, **describe how** the configuration was inspected and the authentication process observed to verify that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  |
| **17.04(6)** | | | |
| For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information. | **Identify** **the documented policies and configuration standards** that define the following:   * Firewall software/hardware is required for all devices (containing personal information) that connect to the Internet when outside the network, and which are also used to access the network. |  |  |
| **17.04(7)** | | | |
| Implement reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are: | |  |
| * Configured to perform automatic updates, and |  |
| * Configured to perform periodic scans. |  |
| **17.04(8)** | | | |
| Educate and train all employees on the proper use of the computer security system and the importance of personal information security. | **Provide the name of the assessor** who attests that the security awareness program was verified to provide awareness to all personnel about the confidential data security policy and procedures. |  |  |

## NRS 603A

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Requirement | Control Effectiveness | Notes |
|  | **NRS 603A.200 Destruction of certain records.** | | |
| D1 | Take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records. |  |  |
|  | **NRS 603A.210 Security measures.** | | |
| S1 | Implement and maintain reasonable security measures to protect personal information from unauthorized access, acquisition, destruction, use, modification or disclosure. |  |  |
| S2 | A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. |  |  |
| S3 | If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section. |  |  |
|  | **NRS 603A.215 Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability.** | | |
| C1 | If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization. |  |  |
| C2 | A data collector doing business in this State to whom subsection 1 does not apply shall not:  (a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or  (b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information. |  |  |
|  | **NRS 603A.220 Disclosure of breach of security of system data; methods of disclosure.** | | |
| B1 | Disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. |  |  |
| B2 | Notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. |  |  |

## NRS 603A

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NRS 603A Requirement** | **Reporting Instruction** | **Assessor’s Response** | | **Control Effectiveness** |
| **NRS 603A.200 Destruction of certain records.** | | | | |
| **D1** | | | | |
| Take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records. | **Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all confidential data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. * Specific requirements for retention of confidential data. * Processes for secure deletion of confidential data when no longer needed for legal, regulatory, or business reasons. * A quarterly process for identifying and securely deleting stored confidential data that exceeds defined retention requirements. |  |  | |
| **NRS 603A.210 Security measures.** | | | | |
| **S1** | | | | |
| Implement and maintain reasonable security measures to protect personal information from unauthorized access, acquisition, destruction, use, modification or disclosure. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  | |
| **S2** | | | | |
| A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s confidential data or sensitive authentication data, or manages the customer's confidential data environment on behalf of a customer. |  |  | |
| **S3** | | | | |
| If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section. | **Identify** how the data collection company is in compliance with state or federal law. |  |  | |
| **NRS 603A.215 Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability.** | | | | |
| **C1** | | | | |
| If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization. | **Identify** the current PCI DSS version the data collection company is compliant with. |  |  | |
| **C2** | | | | |
| A data collector doing business in this State to whom subsection 1 does not apply shall not:  (a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or  (b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information. | **Identify** all locations where confidential data is transmitted or received over open, public networks. |  |  | |
| **Identify** **the documented standards** examined. |  |
| **Describe how** the documented standards were examined and compared to system configurations to verify the use of: | |
| * Security protocols observed in use |  |
| * Strong cryptography for all locations |  |
| **NRS 603A.220 Disclosure of breach of security of system data; methods of disclosure.** | | | | |
| **B1** | | | | |
| Disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  |  | |
| **B2** | | | | |
| Notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  |  | |

## Red Flags Rule

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Requirement | Control Effectiveness | Notes |
| B1 | Obtain approval of the initial written Program by the board of directors or a committee of the board, ensuring oversight of the development, implementation and administration of the Program, training staff, and overseeing service provider arrangements. |  |  |
|  | **Four Basic Elements of the Identity Theft Program** | | |
| E1 | Identity Theft Program must identify relevant Red Flags for covered accounts, including at least the following:  (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;  (2) The presentation of suspicious documents;  (3) The presentation of suspicious personal identifying information, such as a suspicious address change;  (4) The unusual use of, or other suspicious activity related to, a covered account; and  (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor. |  |  |
| E2 | Identity Theft Program must detect Red Flags that have been incorporated into the Program, through methods such as:  (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and  (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts. |  |  |
| E3 | Identity Theft Program must respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft. Examples of responses include:  (a) Monitoring a covered account for evidence of identity theft;  (b) Contacting the customer;  (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;  (d) Reopening a covered account with a new account number;  (e) Not opening a new covered account;  (f) Closing an existing covered account;  (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;  (h) Notifying law enforcement; or  (i) Determining that no response is warranted under the particular circumstances. |  |  |
| E4 | Identity Theft Program must be updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft. Examples of events that indicate an update is needed include:  (a) The experiences of the financial institution or creditor with identity theft;  (b) Changes in methods of identity theft;  (c) Changes in methods to detect, prevent, and mitigate identity theft;  (d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and  (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements. |  |  |
|  | **Administering the Identity Theft Program** | | |
| A1 | Identity Theft Program includes oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management. This oversight includes:  (1) Assigning specific responsibility for the Program’s implementation;  (2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and  (3) Approving material changes to the Program as necessary to address changing identity theft risks. |  |  |
| A2 | Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part. |  |  |
| A3 | The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management’s response; and recommendations for material changes to the Program. |  |  |
| A4 | Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider’s activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft. |  |  |

## PCI DSS v3.1

### Build and Maintain a Secure Network and Systems

#### Requirement 1: Install and maintain a firewall configuration to protect cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings** (check one) | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | **N/A** | **Not Tested** | **Not in Place** |
| **1.1** Establish and implement firewall and router configuration standards that include the following: | | | | | | | | |
| **1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows: | | | | | | | | |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all:   * Network connections, and * Changes to firewall and router configurations. | **Identify the document(s)** reviewed to verify procedures define the formal processes for: | | | | | | | |
| * Testing and approval of all network connections. |  | | | | | | |
| * Testing and approval of all changes to firewall and router configurations. |  | | | | | | |
| **1.1.1.b** For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested. | **Identify the sample of records** for network connections that were examined. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that network connections were approved and tested. |  | | | | | | |
| **Describe how** the sampled records were examined to verify that network connections were: | | | | | | | |
| * Approved |  | | | | | | |
| * Tested |  | | | | | | |
| **1.1.1.c** Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested. | **Identify** **the sample of records** for firewall and router configuration changes that were examined. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that changes made to firewall and router configurations were approved and tested. |  | | | | | | |
| **Describe how** change records were compared to actual changes made to firewall and router configurations to verify the changes were: | | | | | | | |
| * Approved |  | | | | | | |
| * Tested |  | | | | | | |
| **1.1.2** Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to the cardholder data environment, including any wireless networks. | **Identify the current network diagram**(s) examined. |  | | | | | | |
| **Describe how** network connections were observed and compared to the diagram(s) to verify that the diagram: | | | | | | | |
| * Is current. |  | | | | | | |
| * Includes all connections to cardholder data. |  | | | | | | |
| * Includes any wireless network connections. |  | | | | | | |
| **1.1.2.b** Interview responsible personnel to verify that the diagram is kept current. | **Identify** **the document** examined to verify processes require that the network diagram is kept current. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that the diagram is kept current. |  | | | | | | |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.3.a** Examine data flow diagram and interview personnel to verify the diagram:   * Shows all cardholder data flows across systems and networks. * Is kept current and updated as needed upon changes to the environment. | **Identify** **the data-flow diagram**(s) examined. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify the diagram: | | | | | | | |
| * Shows all cardholder data flows across systems and networks. |  | | | | | | |
| * Is kept current and updated as needed upon changes to the environment. |  | | | | | | |
| **1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.4.a** Examine thefirewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. | **Identify** **the firewall configuration standards document** examined to verify requirements for a firewall:   * At each Internet connection. * Between any DMZ and the internal network zone. |  | | | | | | |
| **1.1.4.b** Verify that the current network diagram is consistent with the firewall configuration standards. | **Provide the name of the assessor** who attests that the current network diagram identified at 1.1.2.a was compared to the firewall configuration standards identified at 1.1.4.a to verify they are consistent with each other. |  | | | | | | |
| **1.1.4.c** Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams. | **Describe how** network configurations were observed to verify that, per the documented configuration standards and network diagrams, a firewall is in place: | | | | | | | |
| * At each Internet connection. |  | | | | | | |
| * Between any DMZ and the internal network zone. |  | | | | | | |
| **1.1.5** Description of groups, roles, and responsibilities for management of network components. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify they include a description of groups, roles and responsibilities for management of network components. |  | | | | | | |
| **1.1.5.b** Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented. | **Identify the personnel** responsible for management of network components interviewed for this testing procedure. |  | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that roles and responsibilities are assigned as documented for management of firewall and router components. |  | | | | | | |
| **1.1.6** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.  Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols. | **Identify** **the firewall configuration standards document(s)** reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification for each. |  | | | | | | |
| **Identify** **the router configuration standards document(s)** reviewed to verify the document contains a list of all services, protocols and ports necessary for business, including a business justification for each. |  | | | | | | |
| **1.1.6.b** Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. | **Indicate whether** any insecure services, protocols or ports are allowed. **(yes/no)** |  | | | | | | |
| If “yes,” complete the instructions below for EACH insecure service, protocol, and port allowed: (add rows as needed) | | | | | | | |
| **Identify** the documented justification. |  | | | | | | |
| **Identify the firewall and router configuration standards** reviewed to verify that security features are documented for each insecure service/protocol/port. |  | | | | | | |
| **1.1.6.c** Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port. | If “yes” at 1.1.6.b, complete the following for each insecure service, protocol, and/or port present (add rows as needed): | | | | | | | |
| **Describe how** the firewall and router configurations were examined to verify that the documented security features are implemented for each insecure service, protocol and/or port. |  | | | | | | |
| **1.1.7** Requirement to review firewall and router rule sets at least every six months. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.7.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. | **Identify** **the firewall and router configuration standards** reviewed to verify they require a review of firewall rule sets at least every six months. |  | | | | | | |
| **1.1.7.b** Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. | **Identify the document(s) relating to rule set reviews** that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | | |
| **Identify the responsible personnel interviewed** who confirm that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | | |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.  **Note:** An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. | | | | | | | | |
| **1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment: | | | | | | | | |
| **1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. | | | ☐ | | ☐ | ☐ | ☐ | ☐ |
| **1.2.1.a**  Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment. | **Identify the firewall and router configuration standards** reviewed to verify they identify inbound and outbound traffic necessary for the cardholder data environment. |  | | | | | | |
| **1.2.1.b** Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment. | **Describe how** firewall and router configurations were examined to verify that the following traffic is limited to that which is necessary for the cardholder data environment: | | | | | | | |
| * Inbound traffic |  | | | | | | |
| * Outbound traffic |  | | | | | | |
| **1.2.1.c** Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement. | **Describe how** firewall and router configurations were examined to verify the following is specifically denied: | | | | | | | |
| * All other inbound traffic |  | | | | | | |
| * All other outbound traffic |  | | | | | | |
| **1.2.2** Secure and synchronize router configuration files. | | | ☐ | | ☐ | ☐ | ☐ | ☐ |
| **1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access. | **Describe how** router configuration files were examined to verify they are secured from unauthorized access. |  | | | | | | |
| **1.2.2.b** Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted). | **Describe how** router configuration files were examined to verify they are synchronized. |  | | | | | | |
| **1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment. | **Describe how** firewall and router configurations were examined to verify perimeter firewalls are in place between all wireless networks and the cardholder data environment. |  | | | | | | |
| **1.2.3.b** Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | **Indicate whether** traffic between the wireless environment and the cardholder data environment is necessary for business purposes. **(yes/no)** |  | | | | | | |
| *If “no”:* | | | | | | | |
| **Describe how** firewall and/or router configurations were observed to verify firewalls deny all traffic from any wireless environment into the cardholder environment. |  | | | | | | |
| *If “yes”:* | | | | | | | |
| **Describe how** firewall and/or router configurations were observed to verify firewalls permit only authorized traffic from any wireless environment into the cardholder environment. |  | | | | | | |
| **1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment. | | | | | | | | |
| **1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment: | | | | | | | | |
| **1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | **Describe how** the firewall and router configurations were examined to verify that the DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. |  | | | | | | |
| **1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ. | **Describe how** thefirewall and router configurations were examined to verify that configurations limit inbound Internet traffic to IP addresses within the DMZ. |  | | | | | | |
| **1.3.3** Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.3** Examine firewall and router configurations to verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment. | **Describe how** the examined firewall and router configurations were observed to prevent direct connections between the Internet and the cardholder data environment: | | | | | | | |
| * Inbound |  | | | | | | |
| * Outbound |  | | | | | | |
| **1.3.4** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.  (For example, block traffic originating from the Internet with an internal source address) | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.4** Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ**.** | **Describe how** firewall and router configurations were examined to verify that anti-spoofing measures are implemented. |  | | | | | | |
| **Describe** the anti-spoofing measures implemented |  | | | | | | |
| **1.3.5** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.5** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. | **Describe how** firewall and router configurations were examined to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. |  | | | | | | |
| **1.3.6** Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.) | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.6** Examine firewall and router configurations to verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.) | **Describe how** firewall and router configurations were examined to verify that the firewall performs stateful inspection. |  | | | | | | |
| **Describe** how observed firewall configurations implement stateful inspection |  | | | | | | |
| **1.3.7** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.7** Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. | **Indicate whether** any system components store cardholder data. **(yes/no)** |  | | | | | | |
| *If “yes”:* | | | | | | | |
| **Describe how** firewall and router configurations were examined to verify that the system components that store cardholder data are located on an internal network zone, and are segregated from the DMZ and other untrusted networks. |  | | | | | | |
| **1.3.8** Do not disclose private IP addresses and routing information to unauthorized parties.  Note: Methods to obscure IP addressing may include, but are not limited to:   * Network Address Translation (NAT), * Placing servers containing cardholder data behind proxy servers/firewalls, * Removal or filtering of route advertisements for private networks that employ registered addressing, * Internal use of RFC1918 address space instead of registered addresses. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.8.a** Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. | **Describe** the methods in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |  | | | | | | |
| **Describe how** firewall and router configurations were examined to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |  | | | | | | |
| **1.3.8.b** Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized. | **Identify the document** reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted. |  | | | | | | |
| For each permitted disclosure, **identify the responsible personnel** interviewed who confirm that the disclosure is authorized. |  | | | | | | |
| **1.4** Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include:   * Specific configuration settings are defined for personal firewall software. * Personal firewall software is actively running. * Personal firewall software is not alterable by users of mobile and/or employee-owned devices. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.4.a** Examinepolicies andconfiguration standards to verify:   * Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the network. * Specific configuration settings are defined for personal firewall software. * Personal firewall software is configured to actively run. * Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. | **Indicate whether** mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network are used to access the organization’s network. **(yes/no)** |  | | | | | | |
| *If “no,”* **identify** **the document** reviewed that explicitly prohibits mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network from being used to access the organization’s network.  *Mark 1.4.b as “not applicable”* |  | | | | | | |
| *If “yes,”* **identify** **the documented policies and configuration standards** that define the following:   * Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network, and which are also used to access the network. * Specific configuration settings are defined for personal firewall software. * Personal firewall software is configured to actively run. * Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. |  | | | | | | |
| **1.4.b** Inspect a sample of mobile and/or employee-owned devices to verify that:   * Personal firewall software is installed and configured per the organization’s specific configuration settings. * Personal firewall software is actively running. * Personal firewall software is not alterable by users of mobile and/or employee-owned devices. | **Identify the sample** of mobile and/or employee-owned devices selected for this testing procedure. |  | | | | | | |
| **Describe how** the sample of mobile and/or employee-owned devices was inspected to verify that personal firewall software is: | | | | | | | |
| * Installed and configured per the organization’s specific configuration settings. |  | | | | | | |
| * Actively running. |  | | | | | | |
| * Not alterable by users of mobile and/or employee-owned devices. |  | | | | | | |
| **1.5** Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed** to verify that security policies and operational procedures for managing firewalls are documented. |  | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing firewalls are:   * In use * Known to all affected parties |  | | | | | | |

#### Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.  This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.a** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) | **Identify the sample** of system components selected. |  | | | | | |
| **Identify** **the vendor manuals and sources on the Internet** used to find vendor-supplied accounts/passwords. |  | | | | | |
| *For each item in the sample*, **describe how** attempts to log on (with system administrator help) to the sample of devices and applications using default vendor-supplied accounts and passwords were performed to verify that all default passwords have been changed. |  | | | | | |
| **2.1.b** For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled. | For each item in the sample of system components indicated at 2.1.a, **describe how** all unnecessary default accounts were verified to be **either**: | | | | | | |
| * Removed |  | | | | | |
| * Disabled |  | | | | | |
| **2.1.c** Interview personnel and examine supporting documentation to verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. | **Identify responsible personnel** interviewed who verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. |  | | | | | |
| **Identify supporting documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the supporting documentation examined verified that: | | | | | | |
| * All vendor defaults are changed before a system is installed on the network. |  | | | | | |
| * Unnecessary default accounts are removed or disabled before a system is installed on the network. |  | | | | | |
| **2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.1.a** Interview responsible personnel and examine supporting documentation to verify that:   * Encryption keys were changed from default at installation * Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. | **Indicate whether** there are wireless environments connected to the cardholder data environment or transmitting cardholder data. **(yes/no)**  *If “no,” mark 2.1.1 as “Not Applicable” and proceed to 2.2.* |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify responsible personnel** interviewed who verify that encryption keys are changed:   * From default at installation * Anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **Identify supporting documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the supporting documentation was examined to verify that encryption keys are changed: | | | | | | |
| * From default at installation |  | | | | | |
| * Anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **2.1.1.b** Interview personnel and examine policies and procedures to verify:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. | **Identify responsible personnel** interviewed who verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. |  | | | | | |
| **Identify policies and procedures** examined to verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. |  | | | | | |
| **2.1.1.c** Examine vendor documentation and login to wireless devices, with system administrator help, to verify:   * Default SNMP community strings are not used. * Default passwords/passphrases on access points are not used. | **Identify** **vendor documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** examined vendor documentation was usedto attempt to login to wireless devices (with system administrator help) to verify: | | | | | | |
| * Default SNMP community strings are not used. |  | | | | | |
| * Default passwords/passphrases on access points are not used. |  | | | | | |
| **2.1.1.d** Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for:   * Authentication over wireless networks * Transmission over wireless networks | **Identify** **vendor documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** wireless configuration settings were observed with examined vendor documentation to verify that firmware on wireless devices is updated to support strong encryption for: | | | | | | |
| * Authentication over wireless networks. |  | | | | | |
| * Transmission over wireless networks. |  | | | | | |
| **2.1.1.e** Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable. | **Identify** **vendor documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** wireless configuration settings were observed with examined vendor documentation to verify other security-related wireless vendor defaults were changed, if applicable. |  | | | | | |
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.  Sources of industry-accepted system hardening standards may include, but are not limited to:   * Center for Internet Security (CIS) * International Organization for Standardization (ISO) * SysAdmin Audit Network Security (SANS) Institute * National Institute of Standards Technology (NIST) | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.a** Examine the organization’s system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. | **Identify** **the documented system configuration standards** for all types of system components examined. |  | | | | | |
| **Identify** **the industry-accepted hardening standards** the system configuration standards were verified to be consistent with. |  | | | | | |
| **2.2.b** Examine policies and interview personnel toverify thatsystem configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. | **Identify** **the policy documentation** verified to define that system configuration standards are updated as new vulnerability issues are identified |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that the process is implemented. |  | | | | | |
| **2.2.c** Examine policies and interview personnel toverify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. | **Identify** **the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify: | | | | | | |
| * System configuration standards are applied when new systems are configured |  | | | | | |
| * System configuration standards are verified as being in place before a system is installed on the network. |  | | | | | |
| **2.2.d** Verify that system configuration standards include the following procedures for all types of system components:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers | **Identify the system configuration standards** for all types of system components that include the following procedures:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers |  | | | | | |
| **2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)  **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server. | **Identify the sample** of system components observed. |  | | | | | |
| *For each item in the sample*, **describe how** system configurations were inspected to verify that only one primary function per server is implemented. |  | | | | | |
| **2.2.1.b** If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device. | **Indicate** **whether** virtualization technologies are used. **(yes/no)** |  | | | | | |
| *If “no,”* **describe how** systems were observed to verify that no virtualization technologies are used. |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify** **the functions** for which virtualization technologies are used. |  | | | | | |
| **Identify the sample** of virtual system components or devices observed. |  | | | | | |
| *For each virtual system component and device in the sample*, **describe how** the system configurations were inspected to verify that only one primary function is implemented per virtual system component or device. |  | | | | | |
| **2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled. | **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample*, **describe how** the enabled system services, daemons, and protocols were inspected to verify that only necessary services or protocols are enabled. |  | | | | | |
| **2.2.2.b** Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards. | *For each item in the sample of system components from 2.2.2.a,* **indicate whether** any insecure services, daemons, or protocols are enabled. **(yes/no)**  *If “no,” mark the remainder of 2.2.2.b and 2.2.3 as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **identify responsible personnel** interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol |  | | | | | |
| **2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.  ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.*  *Effective immediately, new implementations must not use SSL or early TLS.*  *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.3.a** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. | *If “yes” at 2.2.2.b, perform the following:* | | | | | | |
| **Identify** **configuration settings** inspected. |  | | | | | |
| **Describe how** configuration settings were inspected to verify that security features for all insecure services, daemons, or protocols are: | | | | | | |
| * Documented |  | | | | | |
| * Implemented |  | | | | | |
| **2.2.3.b** *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:*  Confirm that the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. | **Indicate whether** the assessed entity includes POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS – for which the entity asserts are not susceptible to any known exploits for those protocols. **(yes/no)**  *If ‘no,’ mark the remainder of 2.2.3.b as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **identify the document(s)** examined to verifythat the entity maintains documentation that verifies the devices are not susceptible to any known exploits for SSL/early TLS. |  | | | | | |
| **2.2.3.c** *For all other environments using SSL and/or early TLS:*  Review the documented Risk Mitigation and Migration Plan to verify it includes:   * Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; * Risk assessment results and risk reduction controls in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; * Overview of migration project plan including target migration completion date no later than 30th June 2016. | **Indicate whether** the assessed entity includes any other environments using SSL and/or early TLS **(yes/no)**  *If ‘no,’ mark the remainder of 2.2.3.c as ‘not applicable.’* |  | | | | | |
| If ‘yes,’ **identify the Risk Mitigation and Migration Plan document(s)** examined to verify that it includes:   * Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; * Risk assessment results and risk reduction controls in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; * Overview of migration project plan including target migration completion date no later than 30th June 2016. |  | | | | | |
| **2.2.4** Configure system security parameters to prevent misuse. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.4.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components. | **Identify the system administrators and/or security managers** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed to verify that they have knowledge of common security parameter settings for system components. |  | | | | | |
| **2.2.4.b** Examine the system configuration standards to verify that common security parameter settings are included. | **Identify** **the system configuration standards** examined to verify that common security parameter settings are included. |  | | | | | |
| **2.2.4.c** Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards. | **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample*, **describe how** the common security parameters were inspected to verify that they are set appropriately and in accordance with the configuration standards. |  | | | | | |
| **2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. | **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample*, **describe how** the configurations were inspected to verify that all unnecessary functionality is removed. |  | | | | | |
| **2.2.5.b**. Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration. | **Describe how** the security parameters were examined with relevant documentation to verify that enabled functions are: | | | | | | |
| * Documented |  | | | | | |
| * Support secure configuration |  | | | | | |
| **2.2.5.c**. Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components. | **Identify** **documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the security parameters were examined with relevant documentation to verify that only documented functionality is present on the sampled system components from 2.2.5.a. |  | | | | | |
| **2.3** Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.  ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.*  *Effective immediately, new implementations must not use SSL or early TLS.*  *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: | **Identify the sample** of system components selected for 2.3.a-2.3.d to verify that non-console administrative access is encrypted |  | | | | | |
| **2.3.a** Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator’s password is requested. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on for each system was observed to verify that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Describe how** system configurations for each system were examined to verify that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Identify** **the strong encryption method** used for non-console administrative access. |  | | | | | |
| **2.3.b** Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** services on systems were reviewed to determine that Telnet and other insecure remote-login commands are not available for non-console access. |  | | | | | |
| **Describe how** parameter files on systems were reviewed to determine that Telnet and other insecure remote-login commands are not available for non-console access. |  | | | | | |
| **2.3.c** Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on to each system was observed to verify that administrator access to any web-based management interfaces was encrypted with strong cryptography. |  | | | | | |
| **Identify** **the strong encryption method** used for any web-based management interfaces. |  | | | | | |
| **2.3.d** Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. | **Identify** **the vendor documentation** examined to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **2.3.e** *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:*  Confirm that the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. | **Indicate whether** the assessed entity includes POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS – for which the entity asserts are not susceptible to any known exploits for those protocols. **(yes/no)**  *If ‘no,’ mark the remainder of 2.3.e as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **identify the document(s)** examined to verifythat the entity maintains documentation that verifies the devices are not susceptible to any known exploits for SSL/early TLS. |  | | | | | |
| **2.3.f** *For all other environments using SSL and/or early TLS:*  Review the documented Risk Mitigation and Migration Plan to verify it includes:   * Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; * Risk assessment results and risk reduction controls in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; * Overview of migration project plan including target migration completion date no later than 30th June 2016. | **Indicate whether** the assessed entity includes any other environments using SSL and/or early TLS **(yes/no)**  *If ‘no,’ mark the remainder of 2.3.f as ‘not applicable.’* |  | | | | | |
| *If ‘yes,’* **identify the Risk Mitigation and Migration Plan document(s)** examined to verify that it includes:   * Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; * Risk assessment results and risk reduction controls in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; * Overview of migration project plan including target migration completion date no later than 30th June 2016. |  | | | | | |
| **2.4** Maintain an inventory of system components that are in scope for PCI DSS. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. | **Describe how** the system inventory was examined to verify that a list of hardware and software components is: | | | | | | |
| * Maintained |  | | | | | |
| * Includes a description of function/use for each |  | | | | | |
| **2.4.b** Interview personnel to verify the documented inventory is kept current. | **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that the documented inventory is kept current. |  | | | | | |
| **2.5** Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for managing vendor defaults and other security parameters are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing vendor defaults and other security parameters are:   * In use * Known to all affected parties |  | | | | | |
| **2.6** Shared hosting providers must protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.6** Perform testing procedures **A.1.1** through **A.1.4** detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities’ (merchants and service providers) hosted environment and data. | **Indicate** **whether** the assessed entity is a shared hosting provider. **(yes/no)** |  | | | | | |
| *If “yes,”* **provide the name of the assessor** who attests that Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers has been completed. |  | | | | | |

### Protect Stored Cardholder Data

#### Requirement 3: Protect stored cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | **N/A** | **Not Tested** | **Not in Place** | |
| **3.1** Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific retention requirements for cardholder data * Processes for secure deletion of data when no longer needed. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.1.a** Examine the data-retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. | **Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. * Specific requirements for retention of cardholder data. * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. |  | | | | | | | |
| **3.1.b** Interview personnel to verify that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. | **Identify the personnel** interviewed who confirm that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. |  | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify the following: | | | | | | | | |
| * All locations of stored cardholder data are included in the data-retention and disposal process. |  | | | | | | | |
| * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. |  | | | | | | | |
| * The quarterly automatic or manual process is performed for all locations of cardholder data. |  | | | | | | | |
| **Describe** the quarterly process in place to identify and securely delete stored cardholder data, including whether it is an automatic or manual process. |  | | | | | | | |
| **3.1.c** For a sample of system components that store cardholder data:   * Examine files and system records to verify that the data stored does not exceed the requirements defined in the data-retention policy. * Observe the deletion mechanism to verify data is deleted securely. | **Identify the sample** of system components selected. |  | | | | | | | |
| *For each item in the sample*, **describe how** files and system records were examined to verify that the data stored does not exceed the requirements defined in the data-retention policy. |  | | | | | | | |
| **Describe how** the deletion mechanism was observed to verify data is deleted securely. |  | | | | | | | |
| **3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.  It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:   * There is a business justification, and * The data is stored securely.   Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. | **Indicate whether** the assessed entity is an issuer or supports issuing service. **(yes/no)** |  | | | | | | | |
| *If “yes,” complete the responses for 3.2.a and 3.2.b and mark 3.2.c and 3.2.d as “Not Applicable.”*  *If “no,” mark the remainder of 3.2.a and 3.2.b as “Not Applicable” and proceed to 3.2.c and 3.2.d.* | | | | | | | | |
| **Identify** **the documentation** reviewed to verify there is a documented business justification for the storage of sensitive authentication data. |  | | | | | | | |
| **Identify** **the interviewed personnel** who confirm there is a documented business justification for the storage of sensitive authentication data. |  | | | | | | | |
| For the interview, **summarize the relevant details** of the business justification described. |  | | | | | | | |
| **3.2.b** For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. | *If “yes” at 3.2.a,* | | | | | | | | |
| **Identify** **data stores** examined. |  | | | | | | | |
| **Identify the system configurations** examined. |  | | | | | | | |
| **Describe how** the data stores and system configurations were examined to verify that the sensitive authentication data is secured. |  | | | | | | | |
| **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization. | **Indicate whether** sensitive authentication data is received. **(yes/no)** |  | | | | | | | |
| *If “yes,” complete 3.2.c and 3.2.d.*  *If “no,” mark the remainder of 3.2.c and 3.2.d as “Not Applicable” and proceed to 3.2.1.* | | | | | | | | |
| **Identify** **the document(s)** reviewed to verify that it defines that data is not retained after authorization. |  | | | | | | | |
| **Describe how** system configurations were examined to verify the data is not retained after authorization. |  | | | | | | | |
| **3.2.d** For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable. | **Identify** **the document(s)** reviewed to verify that it defines processes for securely deleting the data to verify that the data is unrecoverable. |  | | | | | | | |
| **Describe how** the processes for securely deleting the data were examined to verify that the data is unrecoverable. |  | | | | | | | |
| **3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.  **Note:** In the normal course of business, the following data elements from the magnetic stripe may need to be retained:   * The cardholder’s name * Primary account number (PAN) * Expiration date * Service code   To minimize risk, store only these data elements as needed for business. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | **Identify the sample** of system components selected for 3.2.1-3.2.3. |  | | | | | | | |
| *For each data source type below from the sample of system of components examined,* **summarize the specific examples of each data source type observed** to verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | | | |
| * Incoming transaction data |  | | | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | | | |
| * History files |  | | | | | | | |
| * Trace files |  | | | | | | | |
| * Database schemas |  | | | | | | | |
| * Database contents |  | | | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | | | |
| **3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | | | |
| * Incoming transaction data |  | | | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | | | |
| * History files |  | | | | | | | |
| * Trace files |  | | | | | | | |
| * Database schemas |  | | | | | | | |
| * Database contents |  | | | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | | | |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed**. If that type of data source is not present, indicate that in the space. | | | | | | | | |
| * Incoming transaction data |  | | | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | | | |
| * History files |  | | | | | | | |
| * Trace files |  | | | | | | | |
| * Database schemas |  | | | | | | | |
| * Database contents |  | | | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | | | |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.  **Note:** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.3.a** Examine written policies and procedures for masking the display of PANs to verify:   * A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access. * PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN. * All other roles not specifically authorized to see the full PAN must only see masked PANs. | **Identify the document(s)** reviewed to verify that written policies and procedures for masking the displays of PANs include the following:   * A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access. * PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN. * All other roles not specifically authorized to see the full PAN must only see masked PANs. |  | | | | | | | |
| **3.3.b** Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests. | **Describe how** system configurations were examined to verify that: | | | | | | | | |
| * Full PAN is only displayed for users/roles with a documented business need. |  | | | | | | | |
| * PAN is masked for all other requests. |  | | | | | | | |
| **3.3.c** Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see full PAN. | **Describe how** displays of PAN were examined to verify that: | | | | | | | | |
| * PANs are masked when displaying cardholder data. |  | | | | | | | |
| * Only those with a legitimate business need are able to see full PAN. |  | | | | | | | |
| **3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:   * One-way hashes based on strong cryptography, (hash must be of the entire PAN). * Truncation (hashing cannot be used to replace the truncated segment of PAN). * Index tokens and pads (pads must be securely stored). * Strong cryptography with associated key-management processes and procedures.   **Note:** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity’s environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures | **Identify** **the documentation** examined about the system used to protect the PAN. |  | | | | | | | |
| **Briefly describe** the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the PAN. |  | | | | | | | |
| **Identify** which of the following methods is used to render the PAN unreadable:   * One-way hashes based on strong cryptography * Truncation * Index token and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  | | | | | | | |
| **3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). | **Identify** **the sample** of data repositories selected. |  | | | | | | | |
| **Identify** **the tables or files** examined for each item in the sample of data repositories. |  | | | | | | | |
| *For each item in the sample*, **describe how** the table or file was examined to verify the PAN is rendered unreadable. |  | | | | | | | |
| **3.4.c** Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable. | **Identify the sample** of removable media selected. |  | | | | | | | |
| *For each item in the sample*, **describe how** the sample of removable media was examined to confirm that the PAN is rendered unreadable. |  | | | | | | | |
| **3.4.d** Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs. | **Identify the sample** of audit logs selected. |  | | | | | | | |
| *For each item in the sample,* **describe how** the sample of audit logs was examined to confirm that the PAN is rendered unreadable or removed from the logs. |  | | | | | | | |
| **3.4.e** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | **Identify whether** hashed and truncated versions of the same PAN are present in the environment **(yes/no)**  *If ‘no,’* mark 3.4.e as ‘not applicable’ and proceed to 3.4.1. |  | | | | | | | |
| *If ‘yes,’* **describe** the implemented controls examined to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. |  | | | | | | | |
| **3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.4.1.a** If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system’s authentication mechanism (for example, not using local user account databases or general network login credentials). | **Indicate whether** disk encryption is used. **(yes/no)** |  | | | | | | | |
| *If “yes,” complete the remainder of 3.4.1.a, 3.4.1.b, and 3.4.1.c.*  *If “no,” mark the remainder of 3.4.1.a, 3.4.1.b and 3.4.1.c as “Not Applicable.’* | | | | | | | | |
| **Describe** the disk encryption mechanism(s) in use. |  | | | | | | | |
| *For each disk encryption mechanism in use*, **describe how** the configuration was inspected and the authentication process observed to verify that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  | | | | | | | |
| **3.4.1.b** Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls). | **Describe how** processes were observed to verify that cryptographic keys are stored securely. |  | | | | | | | |
| **Identify the personnel** interviewed who confirm that cryptographic keys are stored securely. |  | | | | | | | |
| **3.4.1.c** Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored.  **Note:** If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method. | **Identify** **the configurations** examined. |  | | | | | | | |
| **Describe how** the configurations were examined and the processes observed to verify that cardholder data on removable media is encrypted wherever stored. |  | | | | | | | |
| **3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:  **Note:** This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. | **Identify** **the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. |  | | | | | | | |
| **3.5.1** Restrict access to cryptographic keys to the fewest number of custodians necessary. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary. | **Identify** **user access lists** examined. |  | | | | | | | |
| **Describe how** user access lists were examined to verify that access to keys is restricted to the fewest number of custodians necessary. |  | | | | | | | |
| **3.5.2** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). * As at least two full-length key components or key shares, in accordance with an industry-accepted method.   **Note:** It is not required that public keys be stored in one of these forms. | | | ☐ | ☐ | | ☐ | ☐ | | ☐ |
| **3.5.2.a** Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. | **Identify** **the documented procedures** examined to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. |  | | | | | | | |
| **3.5.2.b** Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one, (or more), of the following form at all times.   * Encrypted with a key-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. | **Provide the name** **of the assessor** who attests that all locations where keys are stored were identified. |  | | | | | | | |
| **Describe how** system configurations and key storage locations were examined to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. |  | | | | | | | |
| **3.5.2.c** Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify:   * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. | **Describe how** system configurations and key storage locations were examined to verify that, wherever key-encrypting keys are used: | | | | | | | | |
| * Key-encrypting keys are at least as strong as the data-encrypting keys they protect |  | | | | | | | |
| * Key-encrypting keys are stored separately from data-encrypting keys. |  | | | | | | | |
| **3.5.3** Store cryptographic keys in the fewest possible locations. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.5.3** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations. | **Describe how** key storage locations were examined and processes were observed to verify that keys are stored in the fewest possible locations. |  | | | | | | | |
| **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:  **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.a *Additional Procedure for service provider assessments only***: If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. | **Indicate whether** the assessed entity is a service provider that shares keys with their customers for transmission or storage of cardholder data. **(yes/no)** |  | | | | | | | |
| *If “yes,”* **Identify** **the document** that the service provider provides to their customers examined to verify that it includes guidance on how to securely transmit, store and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. |  | | | | | | | |
| **3.6.b** Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following: | | | | | | | | | |
| **3.6.1** Generation of strong cryptographic keys. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.1.a** Verify that key-management procedures specify how to generate strong keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to generate strong keys. |  | | | | | | | |
| **3.6.1.b** Observe the method for generating keys to verify that strong keys are generated. | **Describe how** the method for generating keys was observed to verify that strong keys are generated. |  | | | | | | | |
| **3.6.2** Secure cryptographic key distribution. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.2.a** Verify that key-management procedures specify how to securely distribute keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to securely distribute keys. |  | | | | | | | |
| **3.6.2.b** Observe the method for distributing keys to verify that keys are distributed securely. | **Describe how** the method for distributing keys was observed to verify that keys are distributed securely. |  | | | | | | | |
| **3.6.3** Secure cryptographic key storage. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.3.a** Verify that key-management procedures specify how to securely store keys. | **Identify** **the documented key-management procedures examined** to verify procedures specify how to securely store keys. |  | | | | | | | |
| **3.6.3.b** Observe the method for storing keys to verify that keys are stored securely. | **Describe how** the method for storing keys was observed to verify that keys are stored securely. |  | | | | | | | |
| **3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.4.a** Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). | **Identify** **the document** that defines:   * Key cryptoperiod(s) for each key type in use * A process for key changes at the end of the defined cryptoperiod(s) |  | | | | | | | |
| **3.6.4.b** Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s). | **Identify** **personnel interviewed** for this testing procedure who confirm that keys are changed at the end of the defined cryptoperiod(s). |  | | | | | | | |
| **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.  **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.5.a** Verify that key-management procedures specify processes for the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the key-management document** examined to verify that key-management processes specify the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | | | |
| **3.6.5.b** Interview personnel to verify the following processes are implemented:   * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. * Keys are replaced if known or suspected to be compromised. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** that verify the following processes are implemented: | | | | | | | | |
| * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. |  | | | | | | | |
| * Keys are replaced if known or suspected to be compromised. |  | | | | | | | |
| * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | | | |
| **3.6.6** If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.  **Note:** Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.6.a** Verify that manual clear-text key-management procedures specify processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another. | **Indicate** **whether** manual clear-text cryptographic key-management operations are used. **(yes/no)** |  | | | | | | | |
| *If “no,” mark the remainder of 3.6.6.a and 3.6.6.b as “Not Applicable.”*  *If “yes,” complete 3.6.6.a and 3.6.6.b.* | | | | | | | | |
| **Identify the document** examined to verify that manual clear-text key-management procedures define processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials of another. |  | | | | | | | |
| **3.6.6 b** Interview personnel and/or observe processes to verify that manual clear-text keys are managed with:   * Split knowledge, AND * Dual control | **Identify** **the personnel** interviewed for this testing procedure, if applicable. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed and/or describe how** processeswere observed to verify the following processes are implemented: | | | | | | | | |
| * Split knowledge |  | | | | | | | |
| * Dual Control |  | | | | | | | |
| **3.6.7** Prevention of unauthorized substitution of cryptographic keys. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.7.a** Verify that key-management procedures specify processes to prevent unauthorized substitution of keys. | **Identify** **the document** examined to verify that key-management procedures specify processes to prevent unauthorized substitution of keys. |  | | | | | | | |
| **3.6.7.b** Interview personnel and/or observe process to verify that unauthorized substitution of keys is prevented. | **Identify** **the personnel** interviewed for this testing procedure, if applicable. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** **and/or describe how** processes were observed to verify that unauthorized substitution of keys is prevented. |  | | | | | | | |
| **3.6.8** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.8.a** Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Identify** **the document** examined to verify that key-management procedures specify processes for key custodians to acknowledge that they understand and accept their key-custodian responsibilities. |  | | | | | | | |
| **3.6.8.b** Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Describe how** key custodian acknowledgements or other evidence were observed to verify that key custodians have acknowledged that they understand and accept their key-custodian responsibilities. |  | | | | | | | |
| **3.7** Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.7** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are:   * Documented, * In use, and * Known to all affected parties | **Identify** **the document** reviewed to verify that security policies and operational procedures for protecting stored cardholder data are documented. |  | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting stored cardholder data are:   * In use * Known to all affected parties |  | | | | | | | |

#### Requirement 4: Encrypt transmission of cardholder data across open, public networks

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **4.1** Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:   * Only trusted keys and certificates are accepted. * The protocol in use only supports secure versions or configurations. * The encryption strength is appropriate for the encryption methodology in use.   ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.*  *Effective immediately, new implementations must not use SSL or early TLS.*  *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.*  *Examples of open, public networks include but are not limited to:*   * *The Internet* * *Wireless technologies, including 802.11 and Bluetooth* * *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* * *General Packet Radio Service (GPRS)* * *Satellite communications* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where cardholder data is transmitted or received over open, public networks. |  | | | | | |
| **Identify** **the documented standards** examined. |  | | | | | |
| **Describe how** the documented standards were examined and compared to system configurations to verify the use of: | | | | | | |
| * Security protocols observed in use |  | | | | | |
| * Strong cryptography for all locations |  | | | | | |
| **4.1.b** Review documented policies and procedures to verify processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. | **Identify the document** reviewed to verify that processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. |  | | | | | |
| **4.1.c** Select and observe a sample of inbound and outbound transmissions as they occur to verify that all cardholder data is encrypted with strong cryptography during transit. | **Describe** **the sample** of inbound and outbound transmissions observed as they occurred. |  | | | | | |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all cardholder data is encrypted with strong cryptography during transit. |  | | | | | |
| **4.1.d** Examine keys and certificates to verify that only trusted keys and/or certificates are accepted. | *For all instances where cardholder data is transmitted or received over open, public networks:* | | | | | | |
| **Describe the mechanisms** used to ensure that only trusted keys and/or certificates are accepted. |  | | | | | |
| **Describe how** the mechanisms were observed to accept only trusted keys and/or certificates. |  | | | | | |
| **4.1.e** Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. | *For all instances where cardholder data Is transmitted or received over open, public networks,* **describe how** system configurations were observed to verify that the protocol is implemented: | | | | | | |
| * To use only secure configurations. |  | | | | | |
| * Does not support insecure versions or configurations. |  | | | | | |
| **4.1.f** Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) | *For each encryption methodology in use,* | | | | | | |
| **Identify** vendor recommendations/best practices for encryption strength. |  | | | | | |
| **Identify** the encryption strength observed to be implemented. |  | | | | | |
| **4.1.g** For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.  *For example, for browser-based implementations:*   * *“HTTPS” appears as the browser Universal Record Locator (URL) protocol; and* * *Cardholder data is only requested if “HTTPS” appears as part of the URL.* | **Indicate whether** TLS is implemented to encrypt cardholder data over open, public networks in the CDE. **(yes/no)** |  | | | | | |
| *If “yes,” for all instances where TLS is used to encrypt cardholder data over open, public networks,* ***describe how*** *system configurations were examined to verify that TLS is enabled whenever cardholder data is transmitted or received, as follows:* | | | | | | |
| * HTTPS appears as part of the browser URL. |  | | | | | |
| * Cardholder data is only requested if HTTPS appears as part of the URL. |  | | | | | |
| **4.1.h** *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:*  Confirm that the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. | **Indicate whether** the assessed entity includes POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS – for which the entity asserts are not susceptible to any known exploits for those protocols. **(yes/no)**  *If ‘no,’ mark the remainder of 4.1.h as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **identify the document(s)** examined to verifythat the entity maintains documentation that verifies the devices are not susceptible to any known exploits for SSL/early TLS. |  | | | | | |
| **4.1.i** *For all other environments using SSL and/or early TLS:*  Review the documented Risk Mitigation and Migration Plan to verify it includes:   * Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; * Risk assessment results and risk reduction controls in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; * Overview of migration project plan including target migration completion date no later than 30th June 2016. | **Indicate whether** the assessed entity includes any other environments using SSL and/or early TLS **(yes/no)**  *If ‘no,’ mark the remainder of 4.1.i as ‘not applicable.’* |  | | | | | |
| If ‘yes,’ **identify the Risk Mitigation and Migration Plan document(s)** examined to verify that it includes:   * Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; * Risk assessment results and risk reduction controls in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; * Overview of migration project plan including target migration completion date no later than 30th June 2016. |  | | | | | |
| **4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.  **Note:** The use of WEP as a security control is prohibited. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.1** Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified:   * Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. * Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission. | **Identify** all wireless networks transmitting cardholder data or connected to the cardholder data environment. |  | | | | | |
| **Identify the documented standards** examined to verify processes define the following for all wireless networks identified:   * Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. * Weak encryption is not used as a security control for authentication or transmission. |  | | | | | |
| **Describe how** documented standards were examined and compared to system configuration settings to verify the following for all wireless networks identified: | | | | | | |
| * Industry best practices are used to implement strong encryption for authentication and transmission. |  | | | | | |
| * Weak encryption is not used as a security control for authentication or transmission. |  | | | | | |
| **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | **Indicate** **whether** end-user messaging technologies are used to send cardholder data. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 4.2.a as “Not Applicable” and proceed to 4.2.b.*  *If “yes,” complete the following:* | | | | | | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **Describe how** the sample of outbound transmissions observed as they occurred to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **4.2.b** Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. | *If “yes” at 4.2.a:* |  | | | | | |
| **Identify** **the policy document** stating that unprotected PANs must not be sent via end-user messaging technologies. |  | | | | | |
| *If “no” at 4.2.a:* | | | | | | |
| **Identify** **the policy document** that explicitly prohibits PAN from being sent via end-user messaging technologies under any circumstances. |  | | | | | |
| **4.3** Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.3** Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for encrypting transmissions of cardholder data are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for encrypting transmissions of cardholder data are:   * In use * Known to all affected parties |  | | | | | |

### Maintain a Vulnerability Management Program

#### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | | **N/A** | **Not Tested** | **Not in Place** |
| **5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components selected (including all operating system types commonly affected by malicious software). |  | | | | | | | |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  | | | | | | | |
| **5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | | | ☐ | ☐ | | ☐ | | ☐ | ☐ |
| 5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | **Identify** **the vendor documentation** reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  | | | | | | | |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | | | | | | | | |
| * Detect all known types of malicious software, |  | | | | | | | |
| * Remove all known types of malicious software, and |  | | | | | | | |
| * Protect against all known types of malicious software. |  | | | | | | | |
| **5.1.2** For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. | | | ☐ | ☐ | ☐ | | | ☐ | ☐ |
| **5.1.2** Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software. | **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** **and/or describe how processes** were observed to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, and that such systems continue to not require anti-virus software. |  | | | | | | | |
| **5.2** Ensure that all anti-virus mechanisms are maintained as follows:   * Are kept current. * Perform periodic scans. * Generate audit logs which are retained per PCI DSS Requirement 10.7. | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.2.a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up-to-date. | **Identify** **the documented policies and procedures** examined to verify that anti-virus software and definitions are required to be kept up to date. |  | | | | | | | |
| **5.2.b** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are:   * Configured to perform automatic updates, and * Configured to perform periodic scans. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are: | | | | | | | | |
| * Configured to perform automatic updates, and |  | | | | | | | |
| * Configured to perform periodic scans. |  | | | | | | | |
| **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:   * The anti-virus software and definitions are current. * Periodic scans are performed. | **Identify the sample** of system components, including all operating system types commonly affected by malicious software, selected for this testing procedure. |  | | | | | | | |
| **Describe how** system components were examined to verify that: | | | | | | | | |
| * The anti-virus software and definitions are current. |  | | | | | | | |
| * Periodic scans are performed. |  | | | | | | | |
| **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:   * Anti-virus software log generation is enabled, and * Logs are retained in accordance with PCI DSS Requirement 10.7. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, were examined to verify that: | | | | | | | | |
| * Anti-virus software log generation is enabled, and |  | | | | | | | |
| * Logs are retained in accordance with PCI DSS Requirement 10.7. |  | | | | | | | |
| **5.3** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.  **Note:** Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active. | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.3.a** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running. | **Identify** **the sample** of system components selected. |  | | | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, were examined to verify that the anti-virus software is actively running. |  | | | | | | | |
| **5.3.b** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users. | *For each item in the sample from 5.3.a,* **describe how** anti-virus configurations, including the master installation of the software, were examined to verify that the anti-virus software cannot be disabled or altered by users. |  | | | | | | | |
| **5.3.c** Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. | **Identify** **the responsible personnel** interviewed who confirm that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | | | |
| **Describe how** the process was observed to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | | | |
| **5.4** Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.4** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for protecting systems against malware are documented. |  | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting systems against malware are:   * In use * Known to all affected parties |  | | | | | | | |

#### Requirement 6: Develop and maintain secure systems and applications

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | **N/A** | **Not Tested** | **Not in Place** | |
| **6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.  **Note:** Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.  Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.1.a** Examine policies and procedures to verify that processes are defined for the following:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. | **Identify** **the documented policies and procedures** examined to confirm that processes are defined:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. |  | | | | | | | |
| **6.1.b** Interview responsible personnel and observe processes to verify that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. | **Identify the responsible personnel** interviewed who confirm that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | | | |
| **Describe** the processes observed to verify that: | | | | | | | | |
| * New security vulnerabilities are identified. |  | | | | | | | |
| * A risk ranking is assigned to vulnerabilities to include identification of all “high” risk and “critical” vulnerabilities. |  | | | | | | | |
| * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | | | |
| **Identify** the outside sources used. |  | | | | | | | |
| **6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.  **Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **6.2.a** Examine policies and procedures related to security-patch installation to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months). | **Identify** **the documented policies and procedures** related to security-patch installation examined to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame. |  | | | | | | | |
| **6.2.b** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:   * That applicable critical vendor-supplied security patches are installed within one month of release. * All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). | **Identify** **the sample** of system components and related software selected for this testing procedure. |  | | | | | | | |
| **Identify** **the vendor security patch list** reviewed. |  | | | | | | | |
| *For each item in the sample,* **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify that: | | | | | | | | |
| * Applicable critical vendor-supplied security patches are installed within one month of release. |  | | | | | | | |
| * All applicable vendor-supplied security patches are installed within an appropriate time frame. |  | | | | | | | |
| **6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:   * In accordance with PCI DSS (for example, secure authentication and logging). * Based on industry standards and/or best practices. * Incorporate information security throughout the software development life cycle.   **Note**: this applies to all software developed internally as well as bespoke or custom software developed by a third party. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.3.a** Examine written software-development processes to verify that the processes are based on industry standards and/or best practices. | **Identify** **the document** that defines software development processes based on industry standards and/or best practices. |  | | | | | | | |
| **Identify** the industry standards and/or best practices used. |  | | | | | | | |
| **6.3.b** Examine written software development processes to verify that information security is included throughout the life cycle. | **Identify** **the documented software development processes** examined to verify that information security is included throughout the life cycle. |  | | | | | | | |
| **6.3.c** Examine written software development processes to verify that software applications are developed in accordance with PCI DSS. | **Identify** **the documented software development processes** examined to verify that software applications are developed in accordance with PCI DSS. |  | | | | | | | |
| **6.3.d** Interview software developers to verify that written software development processes are implemented. | **Identify** **the software developers** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that written software development processes are implemented. |  | | | | | | | |
| **6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.3.1** Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. | **Identify** **the documented software-development processes** examined to verify processes define that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | | | |
| **6.3.2** Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:   * Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines. * Appropriate corrections are implemented prior to release. * Code review results are reviewed and approved by management prior to release.   **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.  *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.* | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.3.2.a** Examine written software development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. | **Identify** **the documented software-development processes** examined to verify processes define that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | | | |
|  | **Identify** **the responsible personnel** interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | | | |
| **Describe how** all custom application code changes must be reviewed, including whether processes are manual or automated. |  | | | | | | | |
| **6.3.2.b** Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above. | **Identify** **the sample** of recent custom application changes selected for this testing procedure. |  | | | | | | | |
| *For each item in the sample*, **describe how** code review processes were observed to verify custom application code is reviewed as follows: | | | | | | | | |
| * Code changes are reviewed by individuals other than the originating code author. |  | | | | | | | |
| * Code changes are reviewed by individuals who are knowledgeable in code-review techniques and secure coding practices. |  | | | | | | | |
| * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). |  | | | | | | | |
| * Appropriate corrections are implemented prior to release. |  | | | | | | | |
| * Code-review results are reviewed and approved by management prior to release. |  | | | | | | | |
| **6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following: | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4** Examine policies and procedures to verify the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change control procedures related to implementing security patches and software modifications are documented. | **Identify the documented policies and procedures** examined to verify that the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change-control procedures related to implementing security patches and software modifications are documented. |  | | | | | | | |
| **6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.1.a** Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s). | **Identify the network documentation** that illustrates that the development/test environments are separate from the production environment(s). |  | | | | | | | |
| **Describe how** network device configurations were examined to verify that the development/test environments are separate from the production environment(s). |  | | | | | | | |
| **6.4.1.b** Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s). | **Identify the access control settings** examined for this testing procedure. |  | | | | | | | |
| **Describe how** the access control settings were examined to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s). |  | | | | | | | |
| **6.4.2** Separation of duties between development/test and production environments. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.2** Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment. | **Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | | | |
| **Identify the personnel assigned to production environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | | | |
| **Describe how** processes were observed to verify that separation of duties is in place between development/test environments and the production environment. |  | | | | | | | |
| **6.4.3** Production data (live PANs) are not used for testing or development. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development. | **Identify the personnel** interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development. |  | | | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing. |  | | | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development. |  | | | | | | | |
| **6.4.3.b** Examine a sample of test data to verify production data (live PANs) is not used for testing or development. | **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for testing. |  | | | | | | | |
| **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for development. |  | | | | | | | |
| **6.4.4** Removal of test data and accounts before production systems become active. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.4.a** Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active. | **Identify the personnel** interviewed who confirm that test data and accounts are removed before a production system becomes active. |  | | | | | | | |
| **Describe how** testing processes were observed to verify that test data is removed before a production system becomes active. |  | | | | | | | |
| **Describe how** testing processes were observed to verify that test accounts are removed before a production system becomes active. |  | | | | | | | |
| **6.4.4.b** Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active. | **Describe how** a sample of data from production systems recently installed or updated was examined to verify test data is removed before the system becomes active. |  | | | | | | | |
| **Describe how** a sample of accounts from production systems recently installed or updated was examined to verify test accounts are removed before the system becomes active. |  | | | | | | | |
| **6.4.5** Change control procedures for the implementation of security patches and software modifications must include the following: | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.a** Examine documented change-control procedures related to implementing security patches and software modifications and verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  | | | | | | | |
| **6.4.5.b** For a sample of system components, interview responsible personnel to determine recent changes/security patches. Trace those changes back to related change control documentation. For each change examined, perform the following: | **Identify** **the sample** of system components selected. |  | | | | | | | |
| **Identify the responsible personnel** interviewed to determine recent changes/security patches. |  | | | | | | | |
| *For each item in the sample,* **identify** **the sample** of changes and the related change control documentation selected for this testing procedure (through 6.4.5.4) |  | | | | | | | |
| **6.4.5.1** Documentation of impact. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that documentation of impact is included in the change control documentation for each sampled change. |  | | | | | | | |
| **6.4.5.2** Documented change approval by authorized parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that documented approval by authorized parties is present in the change control documentation for each sampled change. |  | | | | | | | |
| **6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that the change control documentation for each sampled change includes evidence that functionality testing is performed to verify that the change does not adversely impact the security of the system. |  | | | | | | | |
| **6.4.5.3.b** For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | | | |
| *For each item in the sample,* **identify** **the sample** of custom code changes and the related change control documentation selected for this testing procedure. |  | | | | | | | |
| **Describe how** the custom code changes were traced back to the identified related change control documentation to verify that the change control documentation for each sampled custom code change includes evidence that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. |  | | | | | | | |
| **6.4.5.4** Back-out procedures. | | | ☐ | ☐ | | ☐ | ☐ | | ☐ |
| **6.4.5.4** Verify that back-out procedures are prepared for each sampled change. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that back-out procedures are prepared for each sampled change and present in the change control documentation for each sampled change. |  | | | | | | | |
| **6.5** Address common coding vulnerabilities in software-development processes as follows:   * Traindevelopers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. * Develop applications based on secure coding guidelines.   **Note:** The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.a** Examine software development policies and procedures to verify that training in secure coding techniques is required for developers, based on industry best practices and guidance. | **Identify** **the document** reviewed to verify that training in secure coding techniques is required for developers. |  | | | | | | | |
| **Identify** the industry best practices and guidance that training is based on. |  | | | | | | | |
| **6.5.b** Interview a sample of developers to verify that they are knowledgeable in secure coding techniques. | **Identify** **the developers** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that they are knowledgeable in secure coding techniques. |  | | | | | | | |
| **6.5.c** Examine records of training to verify that software developers received training on secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. | **Identify the records** **of training** that were examined to verify that software developers received training on secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. |  | | | | | | | |
| **6.5.d.** Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: | **Identify** **the software-development policies and procedures** examined to verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: |  | | | | | | | |
| **Identify** **the responsible personnel** interviewed to verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: |  | | | | | | | |
| **Note:** Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external): | | | | | | | | | |
| **6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.1** Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include:   * Validating input to verify user data cannot modify meaning of commands and queries. * Utilizing parameterized queries. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that injection flaws are addressed by coding techniques that include: | | | | | | | | |
| * Validating input to verify user data cannot modify meaning of commands and queries. |  | | | | | | | |
| * Utilizing parameterized queries. |  | | | | | | | |
| **6.5.2** Buffer overflow. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.2** Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include:   * Validating buffer boundaries. * Truncating input strings. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that buffer overflows are addressed by coding techniques that include: | | | | | | | | |
| * Validating buffer boundaries. |  | | | | | | | |
| * Truncating input strings. |  | | | | | | | |
| **6.5.3** Insecure cryptographic storage. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.3** Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that:   * Prevent cryptographic flaws. * Use strong cryptographic algorithms and keys. | *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that insecure cryptographic storage is addressed by coding techniques that: | | | | | | | | |
| * Prevent cryptographic flaws. |  | | | | | | | |
| * Use strong cryptographic algorithms and keys. |  | | | | | | | |
| **6.5.4** Insecure communications. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.4** Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications. | *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that insecure communications are addressed by coding techniques that properly: | | | | | | | | |
| * Authenticate all sensitive communications. |  | | | | | | | |
| * Encrypt all sensitive communications. |  | | | | | | | |
| **6.5.5** Improper error handling. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.5** Examine-software development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages(for example, by returning generic rather than specific error details). | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that improper error handling is addressed by coding techniques that do not leak information via error messages. |  | | | | | | | |
| **6.5.6** All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.6** Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1. | *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that applications are not vulnerable to “High” vulnerabilities, as identified in PCI DSS Requirement 6.1. |  | | | | | | | |
| **Note:** Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external): | | | | | | | | | |
| **Indicate** **whether** web applications and application interfaces are present. **(yes/no)**  *If “no,”* mark the below 6.5.7-6.5.10 as “Not Applicable.”  *If “yes,”* ***complete the following:*** | |  | | | | | | | |
| **6.5.7** Cross-site scripting (XSS). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.7** Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include:   * Validating all parameters before inclusion. * Utilizing context-sensitive escaping. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that cross-site scripting (XSS) is addressed by coding techniques that include: | | | | | | | | |
| * Validating all parameters before inclusion. |  | | | | | | | |
| * Utilizing context-sensitive escaping. |  | | | | | | | |
| **6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.8** Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that include:   * Proper authentication of users. * Sanitizing input. * Not exposing internal object references to users. * User interfaces that do not permit access to unauthorized functions. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that improper access control is addressed by coding techniques that include: | | | | | | | | |
| * Proper authentication of users. |  | | | | | | | |
| * Sanitizing input. |  | | | | | | | |
| * Not exposing internal object references to users. |  | | | | | | | |
| * User interfaces that do not permit access to unauthorized functions. |  | | | | | | | |
| **6.5.9** Cross-site request forgery (CSRF). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.9** Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. |  | | | | | | | |
| **6.5.10** Broken authentication and session management**.**  **Note:** Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.10** Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include:   * Flagging session tokens (for example cookies) as “secure.” * Not exposing session IDs in the URL. * Incorporating appropriate time-outs and rotation of session IDs after a successful login. | **Indicate whether** this ROC is being completed prior to June 30, 2015**. (yes/no)** |  | | | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date, mark the remainder of 6.5.10 as “Not Applicable.”*  *If “no” OR if the assessed entity has this in place ahead of the requirement’s effective date, complete the following:* | | | | | | | | |
| *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that broken authentication and session management are addressed via coding techniques that protect credentials and session IDs, including: | | | | | | | | |
| * Flagging session tokens (for example cookies) as “secure.” |  | | | | | | | |
| * Not exposing session IDs in the URL. |  | | | | | | | |
| * Implementing appropriate time-outs and rotation of session IDs after a successful login |  | | | | | | | |
| **6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:   * Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.   **Note:** This assessment is not the same as the vulnerability scans performed for Requirement 11.2.   * Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.6** For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows:   * Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. * Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. | For each public-facing web application, **identify which** of the two methods are implemented:   * Web application vulnerability security assessments, AND/OR * Automated technical solution that detects and prevents web-based attacks, such as web application firewalls. |  | | | | | | | |
| *If application vulnerability security assessments are indicated above:* | | | | | | | | |
| **Describe the tools and/or methods** used (manual or automated, or a combination of both). |  | | | | | | | |
| **Identify the organization(s)** confirmed to specialize in application security that is performing the assessments. |  | | | | | | | |
| **Identify the documented processes** that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected * That the application is re-evaluated after the corrections. |  | | | | | | | |
| **Identify the responsible personnel** interviewed who confirm that public-facing web applications are reviewed, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. |  | | | | | | | |
| **Identify the records of application security assessments** examined for this testing procedure. |  | | | | | | | |
| **Describe how** the records of application security assessments were examined to verify that public-facing web applications are reviewed as follows: | | | | | | | | |
| * At least annually. |  | | | | | | | |
| * After any changes. |  | | | | | | | |
| * By an organization that specialized in application security. |  | | | | | | | |
| * That at a minimum, all vulnerabilities in requirement 6.5 are included in the assessment. |  | | | | | | | |
| * That all vulnerabilities are corrected. |  | | | | | | | |
| * That the application is re-evaluated after the corrections. |  | | | | | | | |
| *If an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is indicated above:* | | | | | | | | |
| **Describe** the automated technical solution in use that detects and prevents web-based attacks. |  | | | | | | | |
| **Identify** the responsible personnel interviewed who confirm that the above automated technical solution in use to detect and prevent web-based attacks is in place as follows:   * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | | | |
| **Identify the system configuration settings** examined for this testing procedure. |  | | | | | | | |
| **Describe how** the system configuration settings were examined to verify that the above automated technical solution is use to detect and prevent web-based attacks is in place as follows: | | | | | | | | |
| * Is situated in front of public-facing web applications to detect and prevent web-based attacks. |  | | | | | | | |
| * Is actively running and up-to-date as applicable. |  | | | | | | | |
| * Is generating audit logs. |  | | | | | | | |
| * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | | | |
| **6.7** Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.7** Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for developing and maintaining secure systems and applications are documented. |  | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for developing and maintaining secure systems and applications are:   * In use * Known to all affected parties |  | | | | | | | |

### Implement Strong Access Control Measures

#### Requirement 7: Restrict access to cardholder data by business need to know

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.a** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function. * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  | | | | | |
| **7.1.1** Define access needs for each role, including:   * System components and data resources that each role needs to access for their job function. * Level of privilege required (for example, user, administrator, etc.) for accessing resources. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.1** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | **Identify** **the selected sample** of roles for this testing procedure. |  | | | | | |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | | | | | | |
| * System components and data resources that each role needs to access for their job function. |  | | | | | |
| * Identification of privilege necessary for each role to perform their job function. |  | | | | | |
| **7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.2.a** Interview personnel responsible for assigning access to verify that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.2.b** Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the sample** of user IDs ***with privileged access*** selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed to confirm that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each user ID in the selected sample are: | | | | | | |
| * Necessary for that individual’s job function. |  | | | | | |
| * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.3** Assign access based on individual personnel’s job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.3** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. | **Identify the sample** of user IDs examined for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed who confirm that privileges assigned are based on that individual’s job classification and function. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each user ID in the selected sample are based on an individual’s job classification and function. |  | | | | | |
| **7.1.4** Require documented approval by authorized parties specifying required privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.4** Select a sample of user IDs and compare with documented approvals to verify that:   * Documented approval exists for the assigned privileges. * The approval was by authorized parties. * That specified privileges match the roles assigned to the individual. | **Identify the sample** of user IDs examined for this testing procedure. |  | | | | | |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | | | | | | |
| * Documented approval exists for the assigned privileges. |  | | | | | |
| * The approval was by authorized parties. |  | | | | | |
| * That specified privileges match the roles assigned to the individual. |  | | | | | |
| **7.2** Establish an access control system for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.  This access control system must include the following: | | | | | | | |
| **7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows: | | | | | | | |
| **7.2.1** Coverage of all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.1** Confirm that access control systems are in place on all system components. | **Identify** **vendor documentation** examined. |  | | | | | |
| **Describe how** system settings were examined with the vendor documentation to verify that access control systems are in place on all system components. |  | | | | | |
| **7.2.2** Assignment of privileges to individuals based on job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | **Describe how** system settings were examined with the vendor documentation at 7.2.1 to verify that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  | | | | | |
| **7.2.3** Default “deny-all” setting. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.3** Confirm that the access control systems have a default “deny-all” setting. | **Describe how** system settings were examined with vendor documentation at 7.2.1 to verify that access control systems have a default “deny-all” setting. |  | | | | | |
| **7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.3** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting access to cardholder data are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for restricting access to cardholder data are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 8: Identify and authenticate access to system components

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.a** Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8:   * Assign all users a unique ID before allowing them to access system components or cardholder data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  | | | | | |
| **8.1.b** Verify that procedures are implemented for user identification management, by performing the following: | | | | | | | |
| **8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.1** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data. | **Identify** **the responsible administrative personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that all users are assigned a unique ID for access to system components or cardholder data. |  | | | | | |
| **8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.2** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval. | **Identify** **the sample** of privileged user IDs selected for this testing procedure. |  | | | | | |
| **Identify** **the sample** of general user IDs selected for this testing procedure. |  | | | | | |
| **Describe how** observed system settings and the associated authorizations documented for the user IDs were compared to verify that each ID has been implemented with only the privileges specified on the documented approval: | | | | | | |
| * For the sample of privileged user IDs. |  | | | | | |
| * For the sample of general user IDs. |  | | | | | |
| **8.1.3** Immediately revoke access for any terminated users. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.3.a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** **the sample** of users terminated in the past six months selected. |  | | | | | |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **8.1.3.b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  | | | | | |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  | | | | | |
| **8.1.4** Remove/disable inactive user accounts within 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. | **Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled. |  | | | | | |
| **8.1.5** Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.5.a** Interview personnel and observe processes for managing accounts used by vendors to access, support, or maintain system components to verify that accounts used by vendors for remote access are:   * Disabled when not in use. * Enabled only when needed by the vendor, and disabled when not in use. | **Identify** **the personnel** interviewed who confirm that accounts used by vendors for remote access are:   * Disabled when not in use. * Enabled only when needed by the vendor, and disabled when not in use. |  | | | | | |
| **Describe how** processes for managing accounts used by vendors to access, support, or maintain system components were observed to verify that accounts used by vendors for remote access are: | | | | | | |
| * Disabled when not in use. |  | | | | | |
| * Enabled only when needed by the vendor, and disabled when not in use. |  | | | | | |
| **8.1.5.b** Interview personnel and observe processes to verify that vendor remote access accounts are monitored while being used. | **Identify** **the personnel** interviewed who confirm that accounts used by vendors for remote access are monitored while being used. |  | | | | | |
| **Describe how** processes for managing accounts used by vendors to access, support, or maintain system components were observed to verify that vendor remote access accounts are monitored while being used. |  | | | | | |
| **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that authentication parameters are set to require that user accounts be locked after not more than six invalid logon attempts. |  | | | | | |
| **8.1.6.b** ***Additional procedure for service provider assessments only:*** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **Describe** the implemented processes that were observed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. |  | | | | | |
| **8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that system/session idle time out features have been set to 15 minutes or less. |  | | | | | |
| **8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:   * Something you know, such as a password or passphrase. * Something you have, such as a token device or smart card. * Something you are, such as a biometric. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following:   * Examine documentation describing the authentication method(s) used. * For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s). | **Identify the document** describing the authentication method(s) used that was reviewed to verify that the methods require users to be authenticated using a unique ID and additional authentication for access to the cardholder data environment. |  | | | | | |
| **Describe** the authentication methods used (for example, a password or passphrase, a token device or smart card, a biometric, etc.) for each type of system component. |  | | | | | |
| *For each type of authentication method used and for each type of system component,***describe how** the authentication method was observed to be: | | | | | | |
| * Used for access to the cardholder data environment. |  | | | | | |
| * Functioning consistently with the documented authentication method(s). |  | | | | | |
| **8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.1.a** Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage. | **Identify** **the vendor documentation** reviewed for this testing procedure. |  | | | | | |
| **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample,***describe how** system configuration settings were examined to verify that passwords are protected with strong cryptography during ***transmission***. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were examined to verify that passwords are protected with strong cryptography during ***storage***. |  | | | | | |
| **8.2.1.b** For a sample of system components, examine password files to verify that passwords are unreadable during storage. | *For each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that passwords are unreadable during storage. |  | | | | | |
| **8.2.1.c** For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission. | *For each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that passwords are unreadable during transmission. |  | | | | | |
| **8.2.1.d** ***Additional procedure for service provider assessments only:*** Observe password files to verify that non-consumer customer passwords are unreadable during storage. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that non-consumer customer passwords are unreadable during storage. |  | | | | | |
| **8.2.1.e *Additional procedure for service provider assessments only:*** Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that non-consumer customer passwords are unreadable during transmission. |  | | | | | |
| **8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.2** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. | **Identify the document** examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  | | | | | |
| **Describe** the non-face-to-face methods used for requesting password resets. |  | | | | | |
| **Describe how** security personnel were observed to verify that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  | | | | | |
| **8.2.3** Passwords/phrases must meet the following:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters.   Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.3.a** For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that user password parameters are set to require at least the following strength/complexity: | | | | | | |
| * Require a minimum length of at least seven characters. |  | | | | | |
| * Contain both numeric and alphabetic characters. |  | | | | | |
| **8.2.3.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that non-consumer customer passwords are required to meet at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | *Additional procedure for service provider assessments only:***Identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer passwords are required to meet at least the following strength/complexity:   * A minimum length of at least seven characters. * Non-consumer user passwords are required to contain both numeric and alphabetic characters. |  | | | | | |
| **Describe how** internal processes were reviewed to verify that non-consumer customer passwords are required to meet at least the following strength/complexity: | | | | | | |
| * A minimum length of at least seven characters. |  | | | | | |
| * Non-consumer customer passwords are required to contain both numeric and alphabetic characters. |  | | | | | |
| **8.2.4** Change user passwords/passphrases at least once every 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least once every 90 days. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that user password parameters are set to require users to change passwords at least once every 90 days. |  | | | | | |
| **8.2.4.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that:   * Non-consumer customer user passwords are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that:   * Non-consumer customer user passwords are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change. |  | | | | | |
| **Describe how** internal processes were reviewed to verify that: | | | | | | |
| * Non-consumer customer user passwords are required to change periodically; and |  | | | | | |
| * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change. |  | | | | | |
| **8.2.5** Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. |  | | | | | |
| **8.2.5.b** ***Additional Procedure for service provider assessments only:*** Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords cannot be the same as the previous four passwords. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that new non-consumer customer user passwords cannot be the same as the previous four passwords. |  | | | | | |
| **Describe how** internal processes were reviewed to verify that new non-consumer customer user passwords cannot be the same as the previous four passwords. |  | | | | | |
| **8.2.6** Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use. | **Identify** **the documented password procedures** examined to verify the procedures define that:   * First-time passwords must be set to a unique value for each user. * First-time passwords must be changed after the first use. * Reset passwords must be set to a unique value for each user. * Reset passwords must be changed after the first use. |  | | | | | |
| **Describe how** security personnel were observed to: | | | | | | |
| * Set first-time passwords to a unique value for each new user. |  | | | | | |
| * Set first-time passwords to be changed after first use. |  | | | | | |
| * Set reset passwords to a unique value for each existing user. |  | | | | | |
| * Set reset passwords to be changed after first use. |  | | | | | |
| **8.3** Incorporate two-factor authentication for remote network access originating from outside the network, by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).  **Note:** Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.  Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.a** Examine system configurations for remote access servers and systems to verify two-factor authentication is required for:   * All remote access by personnel. * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). | **Describe how** system configurations for remote access servers and systems were examined to verify two-factor authentication is required for: | | | | | | |
| * All remote access by personnel. |  | | | | | |
| * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). |  | | | | | |
| **8.3.b** Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used. | **Identify the sample of personnel** observed connecting remotely to the network selected. |  | | | | | |
| *For each item in the sample,* **describe how** two-factor authentication was observed to be required for remote access to the network. |  | | | | | |
| **Identify** which two factors are used:   * Something you know * Something you are * Something you have |  | | | | | |
| **8.4** Document and communicate authentication policies and procedures to all users including:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.4.a** Examineprocedures and interview personnel to verify that authentication policies and procedures are distributed to all users. | **Identify** **the documented policies and procedures** examined to verify authentication procedures define that authentication procedures and policies are distributed to all users. |  | | | | | |
| **Identify the personnel** interviewed who confirm that authentication policies and procedures are distributed to all users. |  | | | | | |
| **8.4.b** Review authentication policies and procedures that are distributed to users and verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | **Identify the documented authentication policies and procedures that** **are distributed to users** reviewed to verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * That users should change passwords if there is any suspicion the password could be compromised. |  | | | | | |
| **8.4.c** Interview a sample of users to verify that they are familiar with authentication policies and procedures. | **Identify** **the sample** of users interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that the sampled users are familiar with authentication policies and procedures. |  | | | | | |
| **8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:   * Generic user IDs are disabled or removed. * Shared user IDs do not exist for system administration and other critical functions. * Shared and generic user IDs are not used to administer any system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.a** For a sample of system components, examine user ID lists to verify the following:   * Generic user IDs are disabled or removed. * Shared user IDs for system administration activities and other critical functions do not exist. * Shared and generic user IDs are not used to administer any system components. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** user ID lists for the sample of system components were examined to verify that: | | | | | | |
| * Generic user IDs are disabled or removed. |  | | | | | |
| * Shared user IDs for system administration activities and other critical functions do not exist. |  | | | | | |
| * Shared and generic user IDs are not used to administer any system components. |  | | | | | |
| **8.5.b** Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. | **Identify** **the documented policies and procedures** examined to verify authentication policies/procedures define that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. |  | | | | | |
| **8.5.c** Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. | **Identify** **the system administrators** interviewed who confirm that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. |  | | | | | |
| **8.5.1** ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.  This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.  **Note:** Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.1** ***Additional procedure for service providerassessments only:*** Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer. | *Additional procedure for service provider assessments only*, **indicate whether** this ROC is being completed prior to June 30, 2015**. (yes/no)** |  | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark this as “Not Applicable.”  *If “no” OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | |
| **Identify** **the documented procedures** examined to verify that different authentication credentials are used for access to each customer. |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that different authentication credentials are used for access to each customer. |  | | | | | |
| **8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows:   * Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.6.a** Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. | **Identify** **the documented authentication policies and procedures** examined to verify the procedures for using authentication mechanisms define that:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.6.b** Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts. | **Identify the security personnel** interviewed who confirm that authentication mechanisms are assigned to an account and not shared among multiple accounts. |  | | | | | |
| **8.6.c** Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings and/or physical controls, as applicable, were examined to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:   * All user access to, user queries of, and user actions on databases are through programmatic methods. * Only database administrators have the ability to directly access or query databases. * Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.7.a** Review database and application configuration settings and verify that all users are authenticated prior to access. | **Identify** all databases containing cardholder data. |  | | | | | |
| **Describe how** authentication is managed (for example, via application and/or database interfaces). |  | | | | | |
| **Describe how** database and/or application configuration settings were observed to verify that all users are authenticated prior to access. |  | | | | | |
| **8.7.b** Examine database and application configuration settings to verify thatall user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). | *For each database from 8.7.a:* | | | | | | |
| **Describe how** the database and application configuration settings were examined to verify that only programmatic methods are used for: | | | | | | |
| * All user access to the database |  | | | | | |
| * All user queries of the database |  | | | | | |
| * All user actions on the database |  | | | | | |
| **Describe** the process observed to verify that only programmatic methods are used for: | | | | | | |
| * All user access to the database |  | | | | | |
| * All user queries of the database |  | | | | | |
| * All user actions on the database |  | | | | | |
| **8.7.c** Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators. | *For each database from 8.7.a,* **describe how** database application configuration settings were examined to verify that the following are restricted to only database administrators: | | | | | | |
| * User direct access to databases |  | | | | | |
| * Queries of databases |  | | | | | |
| **8.7.d** Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes). | *For each database from 8.7.a:* | | | | | | |
| * **Identify** applications with access to the database. |  | | | | | |
| * **Describe** the implemented methods for ensuring that application IDs can only be used by the applications. |  | | | | | |
| * **Describe how** database access control settings, database application configuration settings and related application IDs were examined together to verify that application IDs can only be used by the applications. |  | | | | | |
| **8.8** Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.8** Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for identification and authentication are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for identification and authentication are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 9: Restrict physical access to cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | | | | | **Summary of Assessment Findings**  (check one) | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | | **In Place w/CCW** | | **N/A** | **Not Tested** | | | | | | | | **Not in Place** | | |
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | | | | | | | ☐ | | ☐ | | ☐ | ☐ | | | | | | | | ☐ | | |
| **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. * Observe a system administrator’s attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are “locked” to prevent unauthorized use. | **Identify and briefly describe** all of the following with systems in the cardholder data environment: | | | | | | | | | | | | | | | | | | | | | |
| * All computer rooms |  | | | | | | | | | | | | | | | | | | | | |
| * All data centers |  | | | | | | | | | | | | | | | | | | | | |
| * Any other physical areas |  | | | | | | | | | | | | | | | | | | | | |
| *For each area identified (add rows as needed),* complete the following: | | | | | | | | | | | | | | | | | | | | | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  | | | | | | | | | | | | | | | | | | | | |
| **Identify** the randomly selected systems in the cardholder environment for which a system administrator login attempt was observed. |  | | | | | | | | | | | | | | | | | | | | |
| **Describe how** consoles for the randomly selected systems were observed to verify that they are “locked” when not in use to prevent unauthorized use. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.1** Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.  **Note:** “Sensitive areas” refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store. | | | | | | | ☐ | | ☐ | | ☐ | ☐ | | | | | ☐ | | | | | |
| **9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas. | **Describe** the video cameras and/or access control mechanisms observed to monitor the entry/exit points to sensitive areas. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.1.b** Verify that video cameras and/or access control mechanisms are protected from tampering or disabling. | **Describe how** the video cameras and/or access control mechanisms were observed to be protected from tampering and/or disabling. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.1.c** Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months. | **Describe how** the data from video cameras and/or access control mechanisms were observed to be reviewed. |  | | | | | | | | | | | | | | | | | | | | |
| **Describe how** data was observed to be stored for at least three months. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.2** Implement physical and/or logical controls to restrict access to publicly accessible network jacks.  For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. | | | | | | | ☐ | | ☐ | | ☐ | ☐ | | | | | ☐ | | | | | |
| **9.1.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly-accessible network jacks. | **Identify responsible personnel** interviewed who confirm that physical and/or logical controls are in place to restrict access to publicly accessible network jacks. |  | | | | | | | | | | | | | | | | | | | | |
| **Describe** the physical and/or logical controls observed at the locations of publicly accessible network jacks to verify the controls are in place restrict access. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | | | | | | | ☐ | | ☐ | | ☐ | | ☐ | | | | ☐ | | | | | |
| **9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted. | **Describe how** physical access was observed to be restricted to the following: | | | | | | | | | | | | | | | | | | | | | |
| * Wireless access points | |  | | | | | | | | | | | | | | | | | | | |
| * Wireless gateways | |  | | | | | | | | | | | | | | | | | | | |
| * Wireless handheld devices | |  | | | | | | | | | | | | | | | | | | | |
| * Network/communications hardware | |  | | | | | | | | | | | | | | | | | | | |
| * Telecommunication lines | |  | | | | | | | | | | | | | | | | | | | |
| **9.2** Develop procedures to easily distinguish between onsite personnel and visitors, to include:   * Identifying onsite personnel and visitors (for example, assigning badges). * Changes to access requirements. * Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). | | | | | | | ☐ | ☐ | | ☐ | | | ☐ | | ☐ | | | | | | | |
| **9.2.a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | **Identify** **the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | |  | | | | | | | | | | | | | | | | | | | |
| **9.2.b** Examine identification methods (such as ID badges) andobserve processes for identifying and distinguishing between onsite personnel and visitors to verify that:   * Visitors are clearly identified, and * It is easy to distinguish between onsite personnel and visitors. | **Identify** the identification methods examined. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * Visitors are clearly identified, and | |  | | | | | | | | | | | | | | | | | | | |
| * It is easy to distinguish between onsite personnel and visitors. | |  | | | | | | | | | | | | | | | | | | | |
| **9.2.c** Verify that access to the identification process (such as a badge system) is limited to authorized personnel. | **Identify** **the document** that defines that access to the identification process is limited to authorized personnel. | |  | | | | | | | | | | | | | | | | | | | |
| **Describe how** access to the identification process was observed to be limited to authorized personnel. | |  | | | | | | | | | | | | | | | | | | | |
| **9.3** Control physical access for onsite personnel to sensitive areas as follows:   * Access must be authorized and based on individual job function. * Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | ☐ | | | | | | |
| **9.3.a** For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that:   * Access to the sensitive area is authorized. * Access is required for the individual’s job function. | **Identify the sample** of onsite personnel with physical access to sensitive areas interviewed for this testing procedure. | | |  | | | | | | | | | | | | | | | | | | |
| *For all items in the sample,* **describe how** responsible personnel were interviewed and access control lists observed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * Access to the sensitive area is authorized. | | |  | | | | | | | | | | | | | | | | | | |
| * Access is required for the individual’s job function. | | |  | | | | | | | | | | | | | | | | | | |
| **9.3.b** Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access. | **Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access. | | |  | | | | | | | | | | | | | | | | | | |
| **9.3.c** Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas. | **Identify** **the sample** of users recently terminated. | | |  | | | | | | | | | | | | | | | | | | |
| *For all items in the sample,* **provide the name of the assessor** who attests that the access control lists were reviewed to verify the personnel do not have physical access to sensitive areas. | | |  | | | | | | | | | | | | | | | | | | |
| **9.4** Implement procedures to identify and authorize visitors.  Procedures should include the following: | | | | | | | | | | | | | | | | | | | | | | |
| **9.4** Verify that visitor authorization and access controls are in place as follows: | | | | | | | | | | | | | | | | | | | | | | |
| **9.4.1** Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | ☐ | | | | | | | |  |
| **9.4.1.a** Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. | **Describe how** visitor authorization processes were observed to verify that visitors:   * Must be authorized before they are granted access to areas where cardholder data is processed or maintained. * Are escorted at all times within areas where cardholder data is processed and maintained. | | |  | | | | | | | | | | | | | | | | | | |
| **Identify personnel** interviewed who confirm that visitor authorization processes are in place so that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. | | |  | | | | | | | | | | | | | | | | | | |
| **9.4.1.b** Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. | **Describe how** the use of visitor badges or other identification was observed to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. | | |  | | | | | | | | | | | | | | | | | | |
| **9.4.2** Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | ☐ | | | |  |
| **9.4.2.a** Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel. | **Describe how** people within the facility were observed to use visitor badges or other identification. | | | |  | | | | | | | | | | | | | | | | | |
| **Describe how** visitors within the facility were observed to be easily distinguishable from onsite personnel. | | | |  | | | | | | | | | | | | | | | | | |
| **9.4.2.b** Verify that visitor badges or other identification expire. | **Describe how** visitor badges or other identification were verified to expire. | | | |  | | | | | | | | | | | | | | | | | |
| **9.4.3** Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.4.3** Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration. | **Describe how** visitors leaving the facility were observed to verify they are asked to surrender their badge or other identification upon departure or expiration. | | | |  | | | | | | | | | | | | | | | | | |
| **9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.  Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log.  Retain this log for a minimum of three months, unless otherwise restricted by law. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.4.4.a** Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. | **Describe how** it was verified that a visitor log is in use to record physical access to: | | | | | | | | | | | | | | | | | | | | | |
| * The facility. | | | | |  | | | | | | | | | | | | | | | | |
| * Computer rooms and data centers where cardholder data is stored or transmitted. | | | | |  | | | | | | | | | | | | | | | | |
| **9.4.4.b** Verify that the log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. | **Provide the name of the assessor** who attests that the visitor log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. | | | | |  | | | | | | | | | | | | | | | | |
| **9.4.4.c** Verify that the log is retained for at least three months. | **Identify** the defined retention period for visitor logs. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** visitor logs were observed to be retained for at least three months. | | | | |  | | | | | | | | | | | | | | | | |
| **9.5** Physically secure all media. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.5** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). | **Identify the documented procedures for protecting cardholder data** reviewed to verify controls for physically securing all media are defined. | | | | |  | | | | | | | | | | | | | | | | |
| *For all types of media used,* **describe the controls** for physically securing the media used. | | | | |  | | | | | | | | | | | | | | | | |
| **9.5.1** Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.5.1.a** Observe the storage location’s physical security to confirm that backup media storage is secure. | **Identify** **all locations** where backup media is stored. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** it was observed that backup media storage is stored in a secure location. | | | | |  | | | | | | | | | | | | | | | | |
| **9.5.1.b** Verify that the storage location security is reviewed at least annually. | **Identify** **the document** reviewed to verify that the storage location must be reviewed at least annually. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** processes were observed to verify that reviews of the security of each storage location are performed at least annually. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6** Maintain strict control over the internal or external distribution of any kind of media, including the following: | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** media distribution is controlled, including distribution to individuals. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.1** Classify media so the sensitivity of the data can be determined. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6.1** Verify that all media is classified so the sensitivity of the data can be determined. | **Identify the documented policy** reviewed to verify policy defines how media is classified. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** the classifications were observed to be implemented so the sensitivity of the data can be determined. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.2** Send the media by secured courier or other delivery method that can be accurately tracked. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6.2.a** Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. | **Identify** **the personnel** interviewed who confirm that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. | | | | |  | | | | | | | | | | | | | | | | |
| **Identify the record**s examined for this testing procedure. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** offsite tracking records were examined to verify that all media is logged and sent via secured courier or other delivery method that can be tracked. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.2.b** Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented. | **Identify the sample** of recent offsite tracking logs for all media selected. | | | | |  | | | | | | | | | | | | | | | | |
| *For each item in the sample,* **describe how** the offsite tracking logs were reviewed to verify that tracking details are documented. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6.3** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | **Identify** **responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | | | | |  | | | | | | | | | | | | | | | | |
| *For each item in the sample in 9.6.2.b,* **describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | | | | |  | | | | | | | | | | | | | | | | |
| **9.7** Maintain strict control over the storage and accessibility of media. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.7** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. | **Identify the documented policy** **for controlling storage and maintenance of all media** that was reviewed to verify that the policy defines required periodic media inventories. | | | | |  | | | | | | | | | | | | | | | | |
| **9.7.1** Properly maintain inventory logs of all media and conduct media inventories at least annually. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.7.1** Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually. | **Identify the media inventories logs** reviewed. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** the media inventory logs were reviewed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * Media inventory logs of all media were observed to be maintained. | | | | |  | | | | | | | | | | | | | | | | |
| * Media inventories are performed at least annually. | | | | |  | | | | | | | | | | | | | | | | |
| **9.8** Destroy media when it is no longer needed for business or legal reasons as follows: | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.8** Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | | | | |  | | | | | | | | | | | | | | | | |
| **9.8.1** Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.8.1.a** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | **Identify** **personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** the procedures were examined to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. | | | | |  | | | | | | | | | | | | | | | | |
| **9.8.1.b** Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured. | **Describe how** the storage containers used for materials to be destroyed are secured. | | | | |  | | | | | | | | | | | | | | | | |
| **9.8.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.8.2** Verify that cardholder data on electronic media is rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. | | | | |  | | | | | | | | | | | | | | | | |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify the industry-accepted standards** used. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.  **Note:** These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.  **Note:** Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9** Examine documented policies and procedures to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. | **Indicate whether** this ROC is being completed prior to June 30, 2015**. (yes/no)** | | | | |  | | | | | | | | | | | | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9 – 9.9.3.b as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify the documented policies and procedures** examined to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.1** Maintain an up-to-date list of devices. The list should include the following:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9.1.a** Examine the list of devices to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | *If “yes” at 9.9 AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9.1.a -9.9.1.c as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify the documented up-to-date list of devices** examined to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.1.b** Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date. | **Identify the sample** of devices from the list selected for this testing procedure. | | | | |  | | | | | | | | | | | | | | | | |
| *For all items in the sample,* **describe how** the devices and device locations for the sample of devices were observed to verify that the list is accurate and up-to-date. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.1.c** Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc. | **Identify personnel** interviewed for this testing procedure. | | | | |  | | | | | | | | | | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify the list of devices is updated when devices are added, relocated, decommissioned, etc. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.2** Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).  **Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9.2.a** Examine documented procedures to verify processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. | *If “yes” at 9.9 AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9.2.a -9.9.2.b as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify** **the documented procedures** examined to verify that processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.2.b** Interview responsible personnel and observe inspection processes to verify:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. | **Identify** **responsible personnel** interviewed who confirm that:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** inspection processes were observed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * All devices are periodically inspected for evidence of tampering. | | | | |  | | | | | | | | | | | | | | | | |
| * All devices are periodically inspected for evidence of substitution. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.3** Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:   * Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Do not install, replace, or return devices without verification. * Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9.3.a** Review training materials for personnel at point-of-sale locations to verify it includes training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | *If “yes” at 9.9 AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9.3.a -9.9.3.b as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify** **the training materials for personnel at point-of-sale locations** that were reviewed to verify the materials include training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting all suspicious behavior to appropriate personnel (for example, a manager or security officer). * Reporting tampering or substitution of devices. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.3.b** Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | **Identify** **the sample** of personnel at point-of-sale locations interviewed to verify they have received training. | | | | |  | | | | | | | | | | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify interviewees are aware of the procedures for the following: | | | | | | | | | | | | | | | | | | | | | |
| * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. | | | | |  | | | | | | | | | | | | | | | | |
| * Not to install, replace, or return devices without verification. | | | | |  | | | | | | | | | | | | | | | | |
| * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). | | | | |  | | | | | | | | | | | | | | | | |
| * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | | | | |  | | | | | | | | | | | | | | | | |
| **9.10** Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.10** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting physical access to cardholder data are documented. | | | | |  | | | | | | | | | | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for restricting physical access to cardholder data are: | | | | | | | | | | | | | | | | | | | | | |
| * In use | | | | |  | | | | | | | | | | | | | | | | |
| * Known to all affected parties | | | | |  | | | | | | | | | | | | | | | | |

### Regularly Monitor and Test Networks

#### Requirement 10: Track and monitor all access to network resources and cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | | | **In Place w/ CCW** | **N/A** | | **Not Tested** | | | | **Not in Place** |
| **10.1** Implement audit trails to link all access to system components to each individual user. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.1** Verify, through observation and interviewing the system administrator, that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. | **Identify the system administrator(s)** interviewed who confirm that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. |  | | | | | | | | | | | |
| **Describe how** audit trails were observed to verify the following: | | | | | | | | | | | | |
| * Audit trails are enabled and active for system components. |  | | | | | | | | | | | |
| * Access to system components is linked to individual users. |  | | | | | | | | | | | |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events: | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following: | **Identify the responsible personnel** interviewed who confirm the following from 10.2.1-10.2.7 are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  | | | | | | | | | | | |
|  | **Identify the sample of audit logs** observed to verify the following from 10.2.1-10.2.7 are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including.   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  | | | | | | | | | | | |
| **10.2.1** All individual user accesses to cardholder data. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2.1** Verify all individual access to cardholder data is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all individual access to cardholder data is logged. |  | | | | | | | | | | | |
| **10.2.2** All actions taken by any individual with root or administrative privileges. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2.2** Verify all actions taken by any individual with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all actions taken by any individual with root or administrative privileges are logged. |  | | | | | | | | | | | |
| **10.2.3** Access to all audit trails. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2.3** Verify access to all audit trails is logged. | *For all items in the sample at 10.2*, **describe how** configuration settings were observed to verify access to all audit trails is logged. |  | | | | | | | | | | | |
| **10.2.4** Invalid logical access attempts. | | | | ☐ | ☐ | | ☐ | | ☐ | | | | ☐ |
| **10.2.4** Verify invalid logical access attempts are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify invalid logical access attempts are logged. |  | | | | | | | | | | | |
| **10.2.5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.2.5.a** Verify use of identification and authentication mechanisms is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify use of identification and authentication mechanisms is logged. |  | | | | | | | | | | | |
| **10.2.5.b** Verify all elevation of privileges is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all elevation of privileges is logged. |  | | | | | | | | | | | |
| **10.2.5.c** Verify all changes, additions, or deletions to any account with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all changes, additions, or deletions to any account with root or administrative privileges are logged. |  | | | | | | | | | | | |
| **10.2.6** Initialization, stopping, or pausing of the audit logs. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.2.6** Verify the following are logged:   * Initialization of audit logs. * Stopping or pausing of audit logs. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify initialization of audit logs is logged. |  | | | | | | | | | | | |
| *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify stopping and pausing of audit logs is logged. |  | | | | | | | | | | | |
| **10.2.7** Creation and deletion of system-level objects. | | | | ☐ | ☐ | | | ☐ | | ☐ | ☐ | | |
| **10.2.7** Verify creation and deletion of system level objects are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify creation and deletion of system level objects are logged. |  | | | | | | | | | | | |
| **10.3** Record at least the following audit trail entries for all system components for each event: | | | | ☐ | ☐ | | | ☐ | | ☐ | ☐ | | |
| **10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following: | **Identify the responsible personnel** interviewed who confirm that for each auditable event from 10.2.1-10.2.7, the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | | | | | | | |
| **Identify the sample of audit logs** from 10.2.1-10.2.7 observed to verify the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | | | | | | | |
| **10.3.1** User identification | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.1** Verify user identification is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify user identification is included in log entries. |  | | | | | | | | | | | |
| **10.3.2** Type of event | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.2** Verify type of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify type of event is included in log entries. |  | | | | | | | | | | | |
| **10.3.3** Date and time | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.3** Verify date and time stamp is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify date and time stamp is included in log entries. |  | | | | | | | | | | | |
| **10.3.4** Success or failure indication | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.4** Verify success or failure indication is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify success or failure indication is included in log entries. |  | | | | | | | | | | | |
| **10.3.5** Origination of event | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.5** Verify origination of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify origination of event is included in log entries. |  | | | | | | | | | | | |
| **10.3.6** Identity or name of affected data, system component, or resource | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify the identity or name of affected data, system component, or resource is included in log entries. |  | | | | | | | | | | | |
| **10.4** Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.  ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).* | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. | **Identify** the time synchronization technologies in use. (If NTP, include version) |  | | | | | | | | | | | |
| **Identify** **the documented time-synchronization process** that defines processes for ensuring the time synchronization technologies are kept current per PCI DSS Requirements 6.1 and 6.2. |  | | | | | | | | | | | |
| **Describe how** processes were examined to verify that time synchronization technologies are: | | | | | | | | | | | | |
| * Implemented. |  | | | | | | | | | | | |
| * Kept current, per the documented process. |  | | | | | | | | | | | |
| **10.4.1** Critical systems have the correct and consistent time. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. * Systems receive time information only from designated central time server(s). | **Identify** **the documented process for acquiring, distributing, and storing the correct time within the organization** examined to verify that the process defines the following:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. * Systems receive time information only from designated central time server(s). |  | | | | | | | | | | | |
| **10.4.1.b** Observe the time-related system-parameter settings for a sample of system components to verify:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. * Systems receive time only from designated central time server(s). | **Identify the sample** of system components selected for 10.4.1.b-10.4.2.b |  | | | | | | | | | | | |
| *For all items in the sample,* **describe how** the time-related system-parameter settings for the sample of system components were observed to verify: | | | | | | | | | | | | |
| * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. |  | | | | | | | | | | | |
| * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. |  | | | | | | | | | | | |
| * Systems receive time only from designated central time server(s). |  | | | | | | | | | | | |
| **10.4.2** Time data is protected. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data. | **Identify the documented time-synchronization procedures** examined to verify procedures define that:   * Access to time data is restricted to only personnel with a business need to access time data. * Define which personnel have a business need to access time data. |  | | | | | | | | | | | |
| **Identify** **the authorized personnel** interviewed who confirm that personnel with access to time data have a business need to access time data. |  | | | | | | | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** configuration settings were examined to restrict access to time data to only personnel with a documented need. |  | | | | | | | | | | | |
| **10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. | **Identify the documented time-synchronization procedures** examined to verify procedures define that changes to time settings on critical systems must be:   * Logged * Monitored * Reviewed |  | | | | | | | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** configuration settings on the sampled system components were examined to log any changes to time settings on critical systems. |  | | | | | | | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** logs were examined to log any changes to time settings on critical systems. |  | | | | | | | | | | | |
| **Describe how** time synchronization processes were examined to verify changes to time settings on critical systems are: | | | | | | | | | | | | |
| * Logged |  | | | | | | | | | | | |
| * Monitored |  | | | | | | | | | | | |
| * Reviewed |  | | | | | | | | | | | |
| **10.4.3** Time settings are received from industry-accepted time sources. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers). | **Identify** **the document** reviewed to verify it defines that:   * Time settings are configured to either accept time updates from specific, industry-accepted time sources; OR * The updates are encrypted with a symmetric key and access control lists specify the IP addresses of client machines that will be provided with the time updates. |  | | | | | | | | | | | |
| **Identify the sample** of time servers selected. |  | | | | | | | | | | | |
| *For all items in the sample,* **describe how** configuration settings were examined to verify either of the following: | | | | | | | | | | | | |
| * **T**hat the time servers receive time updates from specific, industry-accepted external sources. OR |  | | | | | | | | | | | |
| * That time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines. |  | | | | | | | | | | | |
| **Identify** the industry-accepted time source indicated (if applicable). |  | | | | | | | | | | | |
| **10.5** Secure audit trails so they cannot be altered. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows: | **Identify the system administrators** interviewed who confirm that audit trails are secured so that they cannot be altered as follows (from 10.5.1-10.5.5):   * Only individuals who have a job-related need can view audit trail files. * Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. * Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, including: * That current audit trail files are promptly backed up to the centralized log server or media * The frequency that audit trail files are backed up * That the centralized log server or media is difficult to alter * Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. * Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. |  | | | | | | | | | | | |
| **Identify the sample** of system components selected for this testing procedure from 10.5.1-10.5.5. |  | | | | | | | | | | | |
| **10.5.1** Limit viewing of audit trails to those with a job-related need. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.1** Only individuals who have a job-related need can view audit trail files. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify they restrict viewing of audit trail files to only individuals who have a documented job-related need. |  | | | | | | | | | | | |
| **10.5.2** Protect audit trail files from unauthorized modifications. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify that current audit trail files are protected from unauthorized modifications. (e.g., via access control mechanisms, physical segregation, and/or network segregation). |  | | | | | | | | | | | |
| **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.3** Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. |  | | | | | | | | | | | |
| **Identify and briefly describe** the following: | | | | | | | | | | | | |
| * The centralized log server or media to which audit trail files are backed up. |  | | | | | | | | | | | |
| * How frequently the audit trail files are backed up, and how the frequency is appropriate. |  | | | | | | | | | | | |
| * How the centralized log server or media is difficult to alter. |  | | | | | | | | | | | |
| **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.4** Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify that logs for external-facing technologies are written onto a secure, centralized, internal log server or media. |  | | | | | | | | | | | |
| **Describe how** logs for external-facing technologies are written onto a secure centralized internal log server or media. |  | | | | | | | | | | | |
| **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.5** Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs. | *For each item in the sample at 10.5,* **describe how** the following were examined to verify the use of file-integrity monitoring or change-detection software on logs: | | | | | | | | | | | | |
| * System settings |  | | | | | | | | | | | |
| * Monitored files |  | | | | | | | | | | | |
| * Results from monitoring activities |  | | | | | | | | | | | |
| **Identify** the file-integrity monitoring (FIM) or change-detection software verified to be in use. |  | | | | | | | | | | | |
| **10.6** Review logs and security events for all system components to identify anomalies or suspicious activity.  **Note:** Log harvesting, parsing, and alerting tools may be used to meet this Requirement. | | | | | | | | | | | | | |
| **10.6** Perform the following: | | | | | | | | | | | | | |
| **10.6.1** Review the following at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.6.1.a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | **Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | | | | | | | |
| **Describe** the manual or log tools used for daily review of logs. |  | | | | | | | | | | | |
| **10.6.1.b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | **Identify the personnel** interviewed who confirm that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | | | | | | | |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | | | | | | | | | | | | |
| * All security events. |  | | | | | | | | | | | |
| * Logs of all system components that store, process, or transmit CHD and/or SAD. |  | | | | | | | | | | | |
| * Logs of all critical system components. |  | | | | | | | | | | | |
| * Logs of all servers and system components that perform security functions. |  | | | | | | | | | | | |
| **10.6.2** Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. | **Identify** **the documented security policies and procedures** examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. |  | | | | | | | | | | | |
| **Describe the manual or log tools** defined for periodic review of logs of all other system components. |  | | | | | | | | | | | |
| **10.6.2.b** Examine the organization’s risk assessment documentation and interview personnel to verify that reviews are performed in accordance with organization’s policies and risk management strategy. | **Identify** **the organization’s risk assessment documentation** examined to verify that reviews are performed in accordance with the organization’s policies and risk management strategy. |  | | | | | | | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that reviews are performed in accordance with the organization’s policies and risk management strategy. |  | | | | | | | | | | | |
| **10.6.3** Follow up exceptions and anomalies identified during the review process. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | **Identify** **the documented security policies and procedures** examined to verify that procedures define following up on exceptions and anomalies identified during the review process. |  | | | | | | | | | | | |
| **10.6.3.b** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. | **Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed. |  | | | | | | | | | | | |
| **Identify** **the personnel** interviewed who confirm that follow-up to exceptions and anomalies is performed. |  | | | | | | | | | | | |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.7.a** Examine security policies and procedures to verify that they define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. | **Identify** **the documented security policies and procedures** examined to verify that procedures define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. |  | | | | | | | | | | | |
| **10.7.b** Interview personnel and examine audit logs to verify that audit logs are retained for at least one year. | **Identify** **the personnel** interviewed who confirm that audit logs are retained for at least one year. |  | | | | | | | | | | | |
| **Describe how** the audit logs were examined to verify that audit logs are retained for at least one year. |  | | | | | | | | | | | |
| * 1. **10.7.c** Interview personnel and observe processes to verify that at least the last three months’ logs are immediately available for analysis. | **Identify** **the personnel** interviewed who confirm that at least the last three months’ logs are immediately available for analysis. |  | | | | | | | | | | | |
| **Describe** the processes observed to verify that at least the last three months’ logs are immediately available for analysis. |  | | | | | | | | | | | |
| **10.8** Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.8** Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented. |  | | | | | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for monitoring all access to network resources and cardholder data are:   * In use * Known to all affected parties |  | | | | | | | | | | | |

#### Requirement 11: Regularly test security systems and processes

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.  **Note:** Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.  Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.a** Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis. | **Identify** **the documented policies and procedures** examined to verify processes are defined for detection and identification of authorized and unauthorized wireless access points on a quarterly basis. |  | | | | | |
| **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:   * WLAN cards inserted into system components. * Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). * Wireless devices attached to a network port or network device. | **Describe how** the methodology/processes were verified to be adequate to detect and identify unauthorized wireless access points, including the following: | | | | | | |
| * WLAN cards inserted into system components. |  | | | | | |
| * Portable or mobile devices attached to system components to create a wireless access point. |  | | | | | |
| * Wireless devices attached to a network port or network device. |  | | | | | |
| * Any other unauthorized wireless access point. |  | | | | | |
| **11.1.c If wireless scanning is utilized, e**xamine output from recent wireless scans to verify that:   * Authorized and unauthorized wireless access points are identified, and * The scan is performed at least quarterly for all system components and facilities. | **Indicate whether** wireless scanning is utilized. **(yes/no)**  *If ‘no,’ mark the remainder of 11.1.c as ‘not applicable.’* |  | | | | | |
| *If ‘yes,’* **Identify/describe** the output from recent wireless scans examined to verify that:   * Authorized wireless access points are identified. * Unauthorized wireless access points are identified. * The scan is performed at least quarterly. * The scan covers all system components. * The scan covers all facilities. |  | | | | | |
| **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel. | **Indicate** **whether** automated monitoring is utilized. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 11.1.d as “Not Applicable.”*  *If “yes,” complete the following:* | | | | | | |
| **Identify and describe** any automated monitoring technologies in use. |  | | | | | |
| *For each monitoring technology in use,* **describe how** the technology generates alerts to personnel. |  | | | | | |
| **11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.1** Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. | **Identify** **the documented inventory records** of authorized wireless access points examined to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. |  | | | | | |
| **11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.2.a** Examine the organization’s incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected. | **Identify the Incident Response Plan document** examined that defines and requires response in the event that an unauthorized wireless access point is detected. |  | | | | | |
| **11.1.2.b** Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found. | **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that action is taken when unauthorized wireless access points are found. |  | | | | | |
| *And/or:* | | | | | | |
| **Identify the recent wireless scans** inspected for this testing procedure. |  | | | | | |
| **Describe how** the recent wireless scans and related responses were inspected to verify that action is taken when unauthorized wireless access points are found. |  | | | | | |
| **11.2** Run internal and external network vulnerability scans at least quarterly andafter any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).  **Note:** Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.  For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2** Examine scan reports and supporting documentation toverify that internal and external vulnerability scans are performed as follows: | | | | | | | |
| **11.2.1** Perform quarterly internal vulnerability scans, and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. | **Identify** **the internal vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly internal scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.1.b** Review the scan reports and verify that the scan process includes rescans until all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | **Identify the documented process for quarterly internal scanning** to verify the process defines performing rescans as part of the quarterly internal scan process. |  | | | | | |
| *For each of the four internal quarterly scans indicated at 11.2.1.a*, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes,”* ***describe how*** *rescans were verified to be performed until either:* | | | | | | |
| * Passing results are obtained, or |  | | | | | |
| * All “High” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. |  | | | | | |
| **11.2.1.c** Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Identify the responsible personnel** interviewed who confirm that the scan was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate** **whether** a qualified internal resource performs the scan. **(yes/no)**  *If “no,” mark the remainder of 11.2.1.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the scans demonstrated they are qualified to perform the scans. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.  **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).  Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period. | **Identify** **the external network vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly external vulnerability scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.2.b** Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures). | **Describe how** the results of each quarterly scan were reviewed to verify that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| *For each of the four external quarterly scans indicated at 11.2.2.a*, **indicate whether** a rescan was necessary. **(yes/no)** |  | | | | | |
| *If “yes,”* **describe how** the results of the rescan were reviewed to verify that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| **11.2.2.c** Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV). | **Provide the name of the assessor** who attests that the external scan reports were reviewed and verified to have been completed by a PCI SSC-Approved Scanning Vendor (ASV). |  | | | | | |
| **11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.3.a** Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned. | **Identify the document** reviewed to verify processes are defined for performing internal and external scans after any significant change. |  | | | | | |
| **Identify the change control documentation and scan reports** reviewed for this testing procedure. |  | | | | | |
| **Describe how** the change control documentation and scan reports were inspected and correlated to verify that all system components subject to significant change were scanned after the change. |  | | | | | |
| **11.2.3.b** Review scan reports and verify that the scan process includes rescans until:   * For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. * For internal scans, all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | For all scans reviewed in 11.2.3.a, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes”* – for external scans, **describe how** rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist. |  | | | | | |
| *If “yes”* – for internal scans, **describe how** rescans were performed until either passing results were obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved. |  | | | | | |
| **11.2.3.c** Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Describe how** it was validated that the scan was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate whether** an **i**nternal resource performed the scans. **(yes/no)**  *If “no,” mark the remainder of 11.2.3.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the scans demonstrated they are qualified to perform the scans. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3 Penetration Testing**  ***Note:*** *The update to**Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.1 is in place. Do not answer both v2.0 and 3.1 reporting instructions.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| * 1. **Indicate whether** 11.3 for this ROC is being assessed against PCI DSS v2.0 or v3.1 (either is acceptable until June 30, 2015.) **(2.0/3.1)** | | 3.1 | | | | | |
| ***If assessing against PCI DSS v2.0 for 11.3, please complete the following section in purple:*** | | | | | | | |
| **11.3** Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: | | | ☐ | ☐ | **☑** | ☐ | ☐ |
| **11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. | * **Identify the documented penetration test results** which confirm:  1. Internal penetration tests are performed annually. 2. External penetration tests are performed annually.  * **Identify whether** any significant infrastructure or application upgrade or modification occurred during the past 12 months. * **Identify the documented penetration test results** confirming that penetration tests are performed after:  1. Significant internal infrastructure or application upgrade. 2. Significant external infrastructure or application upgrade. | Not Applicable | | | | | |
| **11.3.b** Verify that noted exploitable vulnerabilities were corrected and testing repeated. | * **Identify whether** any exploitable vulnerabilities were noted in the most recent:  1. Internal penetration test results. 2. External penetration test results.  * **Identify the interviewed personnel** who confirm that all noted exploitable vulnerabilities were corrected. * **Identify the documented penetration test results** confirming that:  1. Testing was repeated. 2. All noted exploitable vulnerabilities were corrected. | Not Applicable | | | | | |
| **11.3.c** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | * **Identify whether** internal and/or external resources perform the penetration tests. * **Identify the interviewed personnel who perform the tests**, and describe how the personnel demonstrated they are qualified to perform the tests. * **Describe how** organizational independence of the tester was observed to exist. | Not Applicable | | | | | |
| **11.3.1** Network-layer penetration tests. | | | ☐ | ☐ | **☑** | ☐ | ☐ |
| **11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems. | * **Identify the documented results from the most recent penetration tests** confirming that:  1. Internal penetration testing includes network-layer penetration tests. 2. External penetration testing includes network-layer penetration tests. 3. The network-layer penetration tests include:    * Components that support network functions    * Operating systems  * **Identify the responsible personnel** interviewed who confirm that:  1. Internal penetration testing includes network-layer penetration tests. 2. External penetration testing includes network-layer penetration tests. 3. The network-layer penetration tests include:    * Components that support network functions    * Operating systems | Not Applicable | | | | | |
| **11.3.2** Application-layer penetration tests. | | | ☐ | ☐ | **☑** | ☐ | ☐ |
| **11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5. | * **Identify the documented results from the most recent penetration tests** confirming that:  1. Internal penetration testing includes application-layer penetration tests. 2. External penetration testing includes application-layer penetration tests. 3. The application-layer tests include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5.  * **Identify the responsible personnel** interviewed who confirm that:  1. Internal penetration testing includes application-layer penetration tests. 2. External penetration testing includes application-layer penetration tests. 3. The application-layer tests include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5. | Not Applicable | | | | | |
| **END OF PCI DSS 2.0, 11.3.** | | | | | | | |
| ***If assessing against PCI DSS v3.1 for 11.3, please complete the following:*** | | | | | | | |
| **11.3** Implement a methodology for penetration testing that includes at least the following:   * Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside of the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results.   **Note:** This update toRequirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. Prior to this date, PCI DSS v2.0 requirements for penetration testing must be followed until version 3 is in place. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3** Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented and includes at least the following:   * Is based on industry-accepted penetration testing approaches. * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results. | **Identify the documented penetration-testing methodology** examined to verify a methodology is implemented that includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
|  | **Identify the responsible personnel** interviewed who confirm the penetration–testing methodology implemented includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
|  | **Describe how** the penetration-testing methodology was examined to verify that the implemented methodology includes at least the following: | | | | | | |
| * Based on industry-accepted penetration testing approaches. |  | | | | | |
| * Coverage for the entire CDE perimeter and critical systems. |  | | | | | |
| * Testing from both inside the network, and from outside of the network attempting to get in. |  | | | | | |
| * Testing to validate any segmentation and scope-reduction controls. |  | | | | | |
| * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. |  | | | | | |
| * Defines network-layer penetration tests to include components that support network functions as well as operating systems. |  | | | | | |
| * Review and consideration of threats and vulnerabilities experienced in the last 12 months. |  | | | | | |
| * Retention of penetration testing results and remediation activities results. |  | | | | | |
| **11.3.1** Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.1.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented external penetration test results** reviewed to verify that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work was reviewed to verify that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Identify whether** any significant external infrastructure or application upgrade or modification occurred during the past 12 months. |  | | | | | |
| **Identify** **the documented penetration test results reviewed** to verify that external penetration tests are performed after significant external infrastructure or application upgrade. |  | | | | | |
| **11.3.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Describe how** it was validated that the test was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate whether** an **i**nternal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.1.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.2** Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented internal penetration test results** reviewed to verify that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work was reviewed to verify that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Indicate whether** any significant internal infrastructure or application upgrade or modification occurred during the past 12 months. **(yes/no)** |  | | | | | |
| **Identify** **the documented internal penetration test results** reviewed to verify that internal penetration tests are performed after significant internal infrastructure or application upgrade. |  | | | | | |
| **11.3.2.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Describe how** it was validated that the test was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate whether** an **i**nternal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.2.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.3** Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.3** Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. | **Identify the documented penetration testing results** examined to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. |  | | | | | |
| **11.3.4** If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.4.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Indicate** **whether** segmentation is used to isolate the CDE from other networks. **(yes/no)**  *If “no,” mark the remainder of 11.3.4.a and 11.3.4.b as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **Describe** segmentation controls examined for this testing procedure. |  | | | | | |
| **Describe how** the segmentation controls and penetration-testing methodology were examined to verify that penetration testing procedures are defined to: | | | | | | |
| * Test all segmentation methods to confirm they are operational and effective. |  | | | | | |
| * Isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.3.4.b** Examine the results from the most recent penetration test to verify that:   * Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Identify the documented results from the most recent penetration test** examined to verify that:   * Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * the penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.4** Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.  Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. | **Identify the network diagrams** examined to verify that techniques are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. |  | | | | | |
| **Identify** the techniques observed to be in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. |  | | | | | |
| **Describe how** system configurations were examined to verify that techniques are in place to monitor all traffic: | | | | | | |
| * At the perimeter of the cardholder data environment. |  | | | | | |
| * At critical points in the cardholder data environment. |  | | | | | |
| **11.4.b** Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. | **Describe how** system configurations for intrusion-detection, and/or intrusion-prevention techniques were examined to verify they are configured to alert personnel of suspected compromises. |  | | | | | |
| **Describe how** alerts to personnel are generated. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the generated alerts are received as intended. |  | | | | | |
| **11.4.c** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | **Identify** **the vendor document(s)** examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques |  | | | | | |
| **Describe how** IDS/IPS configurations were examined and compared to vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are: | | | | | | |
| * Configured per vendor instructions to ensure optimal protection. |  | | | | | |
| * Maintained per vendor instructions to ensure optimal protection. |  | | | | | |
| * Updated per vendor instructions to ensure optimal protection. |  | | | | | |
| **11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.  **Note:** For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.a** Verify the use of a change-detection mechanism within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities.  *Examples of files that should be monitored:*   * *System executables* * *Application executables* * *Configuration and parameter files* * *Centrally stored, historical or archived, log and audit files* * *Additional critical files determined by entity (i.e., through risk assessment or other means)* | **Describe** the change-detection mechanism deployed. |  | | | | | |
| **Identify the results** from monitored files reviewed. |  | | | | | |
| **Describe how** change-detection mechanism settings and results from monitored files were observed to monitor changes to: | | | | | | |
| * Critical system files |  | | | | | |
| * Critical configuration files |  | | | | | |
| * Critical content files |  | | | | | |
| **11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly. | **Describe how** it was verified that the change-detection mechanism is configured to: | | | | | | |
| * Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files. |  | | | | | |
| * Perform critical file comparisons at least weekly. |  | | | | | |
| **11.5.1** Implement a process to respond to any alerts generated by the change-detection solution. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.1** Interview personnel to verify that all alerts are investigated and resolved. | **Identify the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize details of the interview** that verify that all alerts are investigated and resolved. |  | | | | | |
| **11.6** Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.6** Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for security monitoring and testing are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for security monitoring and testing are:   * In use * Known to all affected parties |  | | | | | |

### Maintain an Information Security Policy

#### Requirement 12: Maintain a policy that addresses information security for all personnel

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **12.1** Establish, publish, maintain, and disseminate a security policy. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  | | | | | |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | | | | | | |
| * All relevant personnel. |  | | | | | |
| * All relevant vendors and business partners. |  | | | | | |
| **12.1.1** Review the security policy at least annually and update the policy when business objectives or the risk environment change. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1.1** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | **Identify the document** reviewed to verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. |  | | | | | |
| **Describe how** the information security policy was verified to be: | | | | | | |
| * Reviewed at least annually. |  | | | | | |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  | | | | | |
| **12.2** Implement a risk assessment process, that:   * Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), * Identifies critical assets, threats, and vulnerabilities, and * Results in a formal, documented analysis of risk.   *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.2.a** Verify that an annual risk-assessment process is documented that:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. | **Describe how** it was verified that an annual risk-assessment process is documented that: | | | | | | |
| * Identifies critical assets, threats and vulnerabilities. |  | | | | | |
| * Results in formal, documented analysis of risk. |  | | | | | |
| **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | **Identify the risk assessment result documentation** reviewed to verify that:   * The risk assessment process is performed at least annually. * The risk assessment is performed upon significant changes to the environment. * The documented risk assessment process was followed. |  | | | | | |
| **12.3** Develop usage policies for critical technologies and define proper use of these technologies.  **Note:** Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.  Ensure these usage policies require the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed: | **Identify** critical technologies in use. |  | | | | | |
| **Identify the usage policies for all identified critical technologies** reviewed to verify the following policies (12.3.1-12.3.10) are defined:   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **Identify the responsible** **personnel** interviewed who confirm usage policies for all identified critical technologies are implemented and followed (for 12.3.1–12.3.10):   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.1** Explicit approval by authorized parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.1** Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to include processes for explicit approval from authorized parties to use the technologies. |  | | | | | |
| **12.3.2** Authentication for use of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.2** Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token). | **Provide the name of the assessor** who attests that the usage policies were verified to include processes s for all technology used to be authenticated with user ID and password or other authentication item. |  | | | | | |
| **12.3.3** A list of all such devices and personnel with access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.3** Verify that the usage policies define a list of all devices and personnel authorized to use the devices. | **Provide the name of the assessor** who attests that the usage policies were verified to include processes define a list of all devices and personnel authorized to use the devices. |  | | | | | |
| **12.3.4** A method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.4** Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | **Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine:   * Owner * Contact Information * Purpose |  | | | | | |
| **12.3.5** Acceptable uses of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.5** Verify that the usage policies define acceptable uses for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  | | | | | |
| **12.3.6** Acceptable network locations for the technologies. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.6** Verify that the usage policies define acceptable network locations for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable network locations for the technology. |  | | | | | |
| **12.3.7** List of company-approved products. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.7** Verify that the usage policies include a list of company-approved products. | **Provide the name of the assessor** who attests that the usage policies were verified to include a list of company-approved products. |  | | | | | |
| **12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.8.a** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | **Provide the name of the assessor** who attests that the usage policies were verified to require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. |  | | | | | |
| **12.3.8.b** Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity. | **Describe how** configurations for remote access technologies were examined to verify that remote access sessions will be automatically disconnected after a specific period of inactivity. |  | | | | | |
| **Identify** any remote access technologies in use. |  | | | | | |
| **Identify** the period of inactivity specified. |  | | | | | |
| **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | **Provide the name of the assessor** who attests that the usage policies were verified to require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. |  | | | | | |
| **12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to prohibit copying, moving or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements. | **Provide the name of the assessor** who attests that the usage policies were verified to require, for personnel with proper authorization, the protection of cardholder data in accordance with PCI DSS Requirements. |  | | | | | |
| **12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.4.a** Verify that information security policy and procedures clearly define information security responsibilities for all personnel. | **Identify** **the information security policy and procedures** reviewed to verify that they clearly define information security responsibilities for all personnel. |  | | | | | |
| **12.4.b** Interview a sample of responsible personnel to verify they understand the security policies. | **Identify the responsible personnel** interviewed for this testing procedure who confirm they understand the security policy. |  | | | | | |
| **Provide the name of the assessor** who attests that the interviews of responsible personnel conducted verified that they understand the security policies. |  | | | | | |
| **12.5** Assign to an individual or team the following information security management responsibilities: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5** Examine information security policies and procedures to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: | **Identify** **the information security policies** reviewed to verify the specific and formal assignment of the following (including 12.5.1-12.5.5):   * Information security to a Chief Security Officer or other security-knowledgeable member of management. * Responsibility for establishing, documenting and distributing security policies and procedures. * Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel. * Establishing, documenting, and distributing security incident response and escalation procedures. * Administering user account and authentication management. * Monitoring and controlling all access to data. |  | | | | | |
| **12.5.1** Establish, document, and distribute security policies and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.1** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security policies and procedures. * Documenting security policies and procedures. * Distributing security policies and procedures. |  | | | | | |
| **12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring and analyzing security alerts. * Distributing information to appropriate information security and business unit management personnel. |  | | | | | |
| **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.3** Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security incident response and escalation procedures. * Documenting security incident response and escalation procedures. * Distributing security incident response and escalation procedures. |  | | | | | |
| **12.5.4** Administer user accounts, including additions, deletions, and modifications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.4** Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for administering user account and authentication management. |  | | | | | |
| **12.5.5** Monitor and control all access to data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring all access to data * Controlling all access to data |  | | | | | |
| **12.6** Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.a** Review the security awareness program to verify it provides awareness to all personnel about the importance of cardholder data security. | **Identify the documented security awareness program** reviewed to verify it provides awareness to all personnel about the importance of cardholder data security. |  | | | | | |
| **12.6.b** Examine security awareness program procedures and documentation and perform the following: | **Identify the documented security awareness program procedures and additional documentation** examined to verify that:   * The security awareness program provides multiple methods of communicating awareness and educating personnel. * Personnel attend security awareness training: * Upon hire, and * At least annually * Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. |  | | | | | |
| **12.6.1** Educate personnel upon hire and at least annually.  ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel. |  | | | | | |
| **12.6.1.b** Verify that personnel attend security awareness training upon hire and at least annually. | **Describe how** it was observed that all personnel attend security awareness training: | | | | | | |
| * Upon hire |  | | | | | |
| * At least annually |  | | | | | |
| **12.6.1.c** Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security. | **Identify the sample** of personnel interviewed who confirm they have completed security awareness training. |  | | | | | |
| For the interview, **summarize details of the interview** that verify their awareness of the importance of cardholder data security. |  | | | | | |
| **12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. | **Describe how** it was verified that, per the security awareness program, all personnel: | | | | | | |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  | | | | | |
| * Provide an acknowledgement at least annually. |  | | | | | |
| **12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)  **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. | **Identify the documented policy** reviewed to verify requirement for background checks to be conducted:   * On potential personnel who will have access to cardholder data or the cardholder data environment. * Prior to hiring the personnel. |  | | | | | |
| **Identify the Human Resources personnel** interviewed who confirm background checks are conducted:   * On potential personnel who will have access to cardholder data or the cardholder data environment. * Prior to hiring the personnel. |  | | | | | |
| **Describe how** it was verified that background checks are conducted (within the constraints of local laws): | | | | | | |
| * On potential personnel who will have access to cardholder data or the cardholder data environment. |  | | | | | |
| * Prior to hiring the personnel. |  | | | | | |
| **12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8**Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data (for example, backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.), as follows: | **Identify the documented policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data**, reviewed to verify policy defines the following from 12.8.1–12.8.5:   * Maintain a list of service providers. * Maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer. * Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. * Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. * Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  | | | | | |
| **12.8.1** Maintain a list of service providers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.1** Verify that a list of service providers is maintained. | **Describe how** the documented list of service providers was observed to be maintained (kept up-to-date). |  | | | | | |
| **12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE.  ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.2** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer. |  | | | | | |
| **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Describe how** it was verified that the procedures for proper due diligence prior to engaging a service provider are implemented, as documented in the policies and procedures at 12.8. |  | | | | | |
| **12.8.4** Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.4** Verify that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. | **Describe how** it was verified that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. |  | | | | | |
| **12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.5** Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | **Describe how** it was observed that the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  | | | | | |
| **12.9 *Additional requirement for service providers only*:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.  **Note:** This requirement is a best practice until June 30, 2015, after which it becomes a requirement.  **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.9 *Additional testing procedure for service provider assessments only****:*Review service provider’s policies and procedures and observe templates used for written agreement to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | **Indicate whether** the assessed entity is a service provider. **(yes/no)**  *If “no,” mark the remainder of 12.9 as “Not Applicable.”*  *If “yes”:* |  | | | | | |
| **Indicate whether** this ROC is being completed prior to June 30, 2015. **(yes/no)** |  | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date, mark the remainder of 12.9 as “Not Applicable.”*  *If “no” OR if the assessed entity has this in place ahead of the requirement’s effective date:* | | | | | | |
| **Identify the service provider’s policies and procedures** reviewed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **Describe how** templates used for written agreement were observed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following: | **Identify** **the documented incident response plan and related procedures** examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows from 12.10.1–12.10.6:   * Create the incident response plan to be implemented in the event of system breach. * Test the plan at least annually. * Designate specific personnel to be available on a 24/7 basis to respond to alerts: * 24/7 incident monitoring * 24/7 incident response * Provide appropriate training to staff with security breach response responsibilities. * Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. * Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  | | | | | |
| **12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:   * Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage and responses of all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.1.a** Verify that the incident response plan includes:   * Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures * Data back-up processes * Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). * Coverage and responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  | | | | | |
| **12.10.1.b** Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed. | **Identify the sample** of personnel interviewed who confirm that the documented incident response plan and procedures are followed. |  | | | | | |
| **Identify the sample** of previously reported incidents or alerts reviewed for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** documentation was reviewed to confirm that the documented incident response plan and procedures are followed. |  | | | | | |
| **12.10.2** Test the plan at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.2** Verify that the plan is tested at least annually. | **Describe how** it was observed that the incident response plan is tested at least annually. |  | | | | | |
| **12.10.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes. | **Identify** **the document** requiring 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **Identify the sample** **of responsible personnel** interviewed who confirm 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **Describe how** it was observed that designated personnel are available for 24/7 incident response and monitoring coverage for: | | | | | | |
| * Any evidence of unauthorized activity. |  | | | | | |
| * Detection of unauthorized wireless access points. |  | | | | | |
| * Critical IDS alerts. |  | | | | | |
| * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **12.10.4** Provide appropriate training to staff with security breach response responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.4** Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained. | **Identify the sample of responsible personnel** interviewed who confirm that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Identify the documented policy** reviewed that defines that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Describe how** it was observed that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **12.10.5** Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan. | **Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **Describe how** processes were reviewed to verify that ***responding to*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **12.10.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.6** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | | | | | | |
| * According to lessons learned. |  | | | | | |
| * To incorporate industry developments. |  | | | | | |

## PCI DSS v3.2

### Build and Maintain a Secure Network and Systems

#### Requirement 1: Install and maintain a firewall configuration to protect cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings** (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **1.1** Establish and implement firewall and router configuration standards that include the following: | | | | | | | |
| **1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows: | | | | | | | |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all:   * Network connections, and * Changes to firewall and router configurations. | **Identify the document(s)** reviewed to verify procedures define the formal processes for: | | | | | | |
| * Testing and approval of all network connections. |  | | | | | |
| * Testing and approval of all changes to firewall and router configurations. |  | | | | | |
| **1.1.1.b** For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested. | **Identify the sample of records** for network connections that were selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that network connections were approved and tested. |  | | | | | |
| **Describe how** the sampled records verified that network connections were: | | | | | | |
| * Approved |  | | | | | |
| * Tested |  | | | | | |
| **1.1.1.c** Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested. | **Identify** **the sample of records** for firewall and router configuration changes that were selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that changes made to firewall and router configurations were approved and tested. |  | | | | | |
| **Describe how** the sampled records verified that the firewall and router configuration changes were: | | | | | | |
| * Approved |  | | | | | |
| * Tested |  | | | | | |
| **1.1.2** Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to the cardholder data environment, including any wireless networks. | **Identify the current network diagram**(s) examined. |  | | | | | |
| **Describe how** network configurations verified that the diagram: | | | | | | |
| * Is current. |  | | | | | |
| * Includes all connections to cardholder data. |  | | | | | |
| * Includes any wireless network connections. |  | | | | | |
| **1.1.2.b** Interview responsible personnel to verify that the diagram is kept current. | **Identify** **the responsible personnel** interviewed who confirm that the diagram is kept current. |  | | | | | |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.3.a** Examine data flow diagram and interview personnel to verify the diagram:   * Shows all cardholder data flows across systems and networks. * Is kept current and updated as needed upon changes to the environment. | **Identify** **the data-flow diagram**(s) examined. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that the diagram:   * Shows all cardholder data flows across systems and networks. * Is kept current and updated as needed upon changes to the environment. |  | | | | | |
| **1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.4.a** Examine thefirewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. | **Identify** **the firewall configuration standards document** examined to verify requirements for a firewall:   * At each Internet connection. * Between any DMZ and the internal network zone. |  | | | | | |
| **1.1.4.b** Verify that the current network diagram is consistent with the firewall configuration standards. | **Provide the name of the assessor** who attests that the current network diagram is consistent with the firewall configuration standards. |  | | | | | |
| **1.1.4.c** Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams. | **Describe how** network configurations verified that, per the documented configuration standards and network diagrams, a firewall is in place: | | | | | | |
| * At each Internet connection. |  | | | | | |
| * Between any DMZ and the internal network zone. |  | | | | | |
| **1.1.5** Description of groups, roles, and responsibilities for management of network components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify they include a description of groups, roles and responsibilities for management of network components. |  | | | | | |
| **1.1.5.b** Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented. | **Identify the responsible personnel** interviewed who confirm that roles and responsibilities are assigned as documented. |  | | | | | |
| **1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification and approval for each. |  | | | | | |
| **1.1.6.b** Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. | **Indicate whether** any insecure services, protocols or ports are allowed. **(yes/no)** |  | | | | | |
| If “yes,” complete the instructions below for EACH insecure service, protocol, and port allowed: (add rows as needed) | | | | | | |
| **Identify the firewall and router configuration standards** **document(s)** reviewed to verify that security features are documented for each insecure service/protocol/port. |  | | | | | |
| **1.1.6.c** Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port. | If “yes” at 1.1.6.b, complete the following for each insecure service, protocol, and/or port present (add rows as needed): | | | | | | |
| **Describe how** firewall and router configurations verified that the documented security features are implemented for each insecure service, protocol and/or port. |  | | | | | |
| **1.1.7** Requirement to review firewall and router rule sets at least every six months. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.7.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify they require a review of firewall rule sets at least every six months. |  | | | | | |
| **1.1.7.b** Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. | **Identify the document(s) relating to rule set reviews** that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.  **Note:** An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. | | | | | | | |
| **1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment: | | | | | | | |
| **1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.1.a** Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment. | **Identify the firewall and router configuration standards document(s)** reviewed to verify they identify inbound and outbound traffic necessary for the cardholder data environment. |  | | | | | |
| **1.2.1.b** Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment. | **Describe how** firewall and router configurations verified that the following traffic is limited to that which is necessary for the cardholder data environment: | | | | | | |
| * Inbound traffic |  | | | | | |
| * Outbound traffic |  | | | | | |
| **1.2.1.c** Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement. | **Describe how** firewall and router configurations verified that the following is specifically denied: | | | | | | |
| * All other inbound traffic |  | | | | | |
| * All other outbound traffic |  | | | | | |
| **1.2.2** Secure and synchronize router configuration files. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access. | **Describe how** router configuration files are secured from unauthorized access. |  | | | | | |
| **1.2.2.b** Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted). | **Describe how** router configurations are synchronized. |  | | | | | |
| **1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment. | **Describe how** firewall and router configurations verified that perimeter firewalls are in place between all wireless networks and the cardholder data environment. |  | | | | | |
| **1.2.3.b** Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | **Indicate whether** traffic between the wireless environment and the cardholder data environment is necessary for business purposes. **(yes/no)** |  | | | | | |
| *If “no”:* | | | | | | |
| **Describe how** firewall and/or router configurations verified that firewalls deny all traffic from any wireless environment into the cardholder environment. |  | | | | | |
| *If “yes”:* | | | | | | |
| **Describe how** firewall and/or router configurations verified that firewalls permit only authorized traffic from any wireless environment into the cardholder environment. |  | | | | | |
| **1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment. | | | | | | | |
| **1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment: | | | | | | | |
| **1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | **Describe how** firewall and router configurations verified that the DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. |  | | | | | |
| **1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ. | **Describe how** firewall and router configurations verified that configurations limit inbound Internet traffic to IP addresses within the DMZ. |  | | | | | |
| **1.3.3** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.  (For example, block traffic originating from the Internet with an internal source address) | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.3** Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ**.** | **Describe how** firewall and router configurations verified that anti-spoofing measures are implemented. |  | | | | | |
| **1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.4** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. | **Describe how** firewall and router configurations verified that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. |  | | | | | |
| **1.3.5** Permit only “established” connections into the network. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.5** Examine firewall and router configurations to verify that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session. | **Describe how** firewall and router configurations verified that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session |  | | | | | |
| **1.3.6** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.6** Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. | **Indicate whether** any system components store cardholder data. **(yes/no)** |  | | | | | |
| *If “yes”:* | | | | | | |
| **Describe how** firewall and router configurations verified that the system components that store cardholder data are located on an internal network zone, and are segregated from the DMZ and other untrusted networks. |  | | | | | |
| **1.3.7** Do not disclose private IP addresses and routing information to unauthorized parties.  Note: Methods to obscure IP addressing may include, but are not limited to:   * Network Address Translation (NAT), * Placing servers containing cardholder data behind proxy servers/firewalls, * Removal or filtering of route advertisements for private networks that employ registered addressing, * Internal use of RFC1918 address space instead of registered addresses. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.7.a** Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. | **Describe how** firewall and router configurations verified that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |  | | | | | |
| **1.3.7.b** Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized. | **Identify the document** reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted. |  | | | | | |
| For each permitted disclosure, **identify the responsible personnel** interviewed who confirm that the disclosure is authorized. |  | | | | | |
| **1.4** Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:   * Specific configuration settings are defined. * Personal firewall (or equivalent functionality) is actively running. * Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.4.a** Examinepolicies andconfiguration standards to verify:   * Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. * Specific configuration settings are defined for personal firewall or equivalent functionality. * Personal firewall or equivalent functionality is configured to actively run. * Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices. | **Indicate whether** portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network are used to access the organization’s CDE. **(yes/no)** |  | | | | | |
| *If “no,”* **identify** **the document** reviewed that explicitly prohibits portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network from being used to access the organization’s CDE.  *Mark 1.4.b as “not applicable”* |  | | | | | |
| *If “yes,”* **identify** **the documented policies and configuration standards** that define the following:   * Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. * Specific configuration settings are defined for personal firewall or equivalent functionality. * Personal firewall or equivalent functionality is configured to actively run. * Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices. |  | | | | | |
| **1.4.b** Inspect a sample of portable computing devices (including company and/or employee-owned)to verify that:   * Personal firewall (or equivalent functionality) is installed and configured per the organization’s specific configuration settings. * Personal firewall (or equivalent functionality) is actively running. * Personal firewall or equivalent functionality is not alterable by users of the portable computing devices. | **Identify the sample** of mobile and/or employee-owned devices selected for this testing procedure. |  | | | | | |
| **Describe how** the sample of portable computing devices (including company and/or employee-owned) verified that personal firewall software is: | | | | | | |
| * Installed and configured per the organization’s specific configuration settings. |  | | | | | |
| * Actively running. |  | | | | | |
| * Not alterable by users of mobile and/or employee-owned devices. |  | | | | | |
| **1.5** Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed** to verify that security policies and operational procedures for managing firewalls are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing firewalls are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.  This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.a** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| **Identify** **the vendor manuals and sources on the Internet** used to find vendor-supplied accounts/passwords. |  | | | | | |
| *For each item in the sample*, **describe how** attempts to log on to the sample of devices and applications using default vendor-supplied accounts and passwords verified that all default passwords have been changed. |  | | | | | |
| **2.1.b** For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled. | For each item in the sample of system components indicated at 2.1.a, **describe how** all unnecessary default accounts were verified to be **either**: | | | | | | |
| * Removed |  | | | | | |
| * Disabled |  | | | | | |
| **2.1.c** Interview personnel and examine supporting documentation to verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. | **Identify the responsible personnel** interviewed who verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. |  | | | | | |
| **Identify supporting documentation** examined to verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. |  | | | | | |
| **2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.1.a** Interview responsible personnel and examine supporting documentation to verify that:   * Encryption keys were changed from default at installation * Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. | **Indicate whether** there are wireless environments connected to the cardholder data environment or transmitting cardholder data. **(yes/no)**  *If “no,” mark 2.1.1 as “Not Applicable” and proceed to 2.2.* |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify the responsible personnel** interviewed who verify that encryption keys are changed:   * From default at installation * Anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **Identify supporting documentation** examined to verify that:   * Encryption keys were changed from default at installation * Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **2.1.1.b** Interview personnel and examine policies and procedures to verify:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. | **Identify the responsible personnel** interviewed who verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/passphrases on access points are required to be changed upon installation. |  | | | | | |
| **Identify policies and procedures** examined to verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. |  | | | | | |
| **2.1.1.c** Examine vendor documentation and login to wireless devices, with system administrator help, to verify:   * Default SNMP community strings are not used. * Default passwords/passphrases on access points are not used. | **Identify** **vendor documentation** examined to verify that:   * Default SNMP community strings are not used. * Default passwords/passphrases on access points are not used. |  | | | | | |
| **Describe how** attempts to login to wireless devices verified that: | | | | | | |
| * Default SNMP community strings are not used. |  | | | | | |
| * Default passwords/passphrases on access points are not used. |  | | | | | |
| **2.1.1.d** Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for:   * Authentication over wireless networks * Transmission over wireless networks | **Identify** **vendor documentation** examined to verify firmware on wireless devices is updated to support strong encryption for:   * Authentication over wireless networks * Transmission over wireless networks |  | | | | | |
| **Describe how** wireless configuration settings verified that firmware on wireless devices is updated to support strong encryption for: | | | | | | |
| * Authentication over wireless networks. |  | | | | | |
| * Transmission over wireless networks. |  | | | | | |
| **2.1.1.e** Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable. | **Identify** **vendor documentation** examined to verify other security-related wireless vendor defaults were changed, if applicable. |  | | | | | |
| **Describe how** wireless configuration settings verified that other security-related wireless vendor defaults were changed, if applicable. |  | | | | | |
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.  Sources of industry-accepted system hardening standards may include, but are not limited to:   * Center for Internet Security (CIS) * International Organization for Standardization (ISO) * SysAdmin Audit Network Security (SANS) Institute * National Institute of Standards Technology (NIST) | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.a** Examine the organization’s system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. | **Identify** **the documented system configuration standards** for all types of system components examined to verify the system configuration standards are consistent with industry-accepted hardening standards. |  | | | | | |
| **Provide the name of the assessor** who attests that the system configuration standards are consistent with industry-accepted hardening standards. |  | | | | | |
| **2.2.b** Examine policies and interview personnel toverify thatsystem configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. | **Identify** **the policy documentation** examined toverify thatsystem configuration standards are updated as new vulnerability issues are identified. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm thatsystem configuration standards are updated as new vulnerability issues are identified. |  | | | | | |
| **2.2.c** Examine policies and interview personnel toverify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. | **Identify** **the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. |  | | | | | |
| **2.2.d** Verify that system configuration standards include the following procedures for all types of system components:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers | **Identify the system configuration standards** for all types of system components that include the following procedures:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers |  | | | | | |
| **2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)  **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** system configurations verified that only one primary function per server is implemented. |  | | | | | |
| **2.2.1.b** If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device. | **Indicate** **whether** virtualization technologies are used. **(yes/no)** |  | | | | | |
| *If “no,”* **describe how** systems were observed to verify that no virtualization technologies are used. |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify the sample** of virtual system components or devices selected for this testing procedure. |  | | | | | |
| *For each virtual system component and device in the sample*, **describe how** system configurations verified that only one primary function is implemented per virtual system component or device. |  | | | | | |
| **2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** the enabled system services, daemons, and protocols verified that only necessary services or protocols are enabled. |  | | | | | |
| **2.2.2.b** Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards. | *For each item in the sample of system components from 2.2.2.a,* **indicate whether** any insecure services, daemons, or protocols are enabled. **(yes/no)**  *If “no,” mark the remainder of 2.2.2.b and 2.2.3 as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **identify the responsible personnel** interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol |  | | | | | |
| **2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure  ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.3.a** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. | *If “yes” at 2.2.2.b, perform the following:* | | | | | | |
| **Describe how** configuration settings verified that security features for all insecure services, daemons, or protocols are: | | | | | | |
| * Documented |  | | | | | |
| * Implemented |  | | | | | |
| **2.2.3.b** If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS. | **Indicate whether** SSL/early TLS is used. **(yes/no)**  *If ‘no,’ mark the remainder of 2.2.3.b as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **provide the name of the assessor** who attests that the testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS were performed. |  | | | | | |
| **2.2.4** Configure system security parameters to prevent misuse. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.4.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components. | **Identify the system administrators and/or security managers** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed to verify that they have knowledge of common security parameter settings for system components. |  | | | | | |
| **2.2.4.b** Examine the system configuration standards to verify that common security parameter settings are included. | **Identify** **the system configuration standards** examined to verify that common security parameter settings are included. |  | | | | | |
| **2.2.4.c** Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** the common security parameters verified that they are set appropriately and in accordance with the configuration standards. |  | | | | | |
| **2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** configurations verified that all unnecessary functionality is removed. |  | | | | | |
| **2.2.5.b** Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration. | **Describe how** the security parameters and relevant documentation verified that enabled functions are: | | | | | | |
| * Documented |  | | | | | |
| * Support secure configuration |  | | | | | |
| **2.2.5.c** Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components. | **Identify** **documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the security parameters verified that only documented functionality is present on the sampled system components from 2.2.5.a. |  | | | | | |
| **2.3** Encrypt all non-console administrative access using strong cryptography.  ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: | **Identify the sample** of system components selected for 2.3.a-2.3.d. |  | | | | | |
| **2.3.a** Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator’s password is requested. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on to each system verified that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Describe how** system configurations for each system verified that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Identify** **the strong encryption method** used for non-console administrative access. |  | | | | | |
| **2.3.b** Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** services and parameter files on systems verified that Telnet and other insecure remote-login commands are not available for non-console access. |  | | | | | |
| **2.3.c** Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on to each system verified that administrator access to any web-based management interfaces was encrypted with strong cryptography. |  | | | | | |
| **Identify** **the strong encryption method** used for any web-based management interfaces. |  | | | | | |
| **2.3.d** Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. | **Identify** **the vendor documentation** examined to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **2.3.e** If SSL/early TLS is used, perform testing procedures in *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.* | **Indicate whether** SSL/early TLS is used. **(yes/no)**  *If ‘no,’ mark the remainder of 2.3.e as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **provide the name of the assessor** who attests that the testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS were performed. |  | | | | | |
| **2.4** Maintain an inventory of system components that are in scope for PCI DSS. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. | **Describe how** the system inventory verified that a list of hardware and software components is: | | | | | | |
| * Maintained |  | | | | | |
| * Includes a description of function/use for each |  | | | | | |
| **2.4.b** Interview personnel to verify the documented inventory is kept current. | **Identify** **the responsible personnel** interviewed who confirm that the documented inventory is kept current. |  | | | | | |
| **2.5** Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for managing vendor defaults and other security parameters are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing vendor defaults and other security parameters are:   * In use * Known to all affected parties |  | | | | | |
| **2.6** Shared hosting providers must protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.6** Perform testing procedures **A1.1** through **A1.4** detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities’ (merchants and service providers) hosted environment and data. | **Indicate** **whether** the assessed entity is a shared hosting provider. **(yes/no)** |  | | | | | |
| *If “yes,”* **provide the name of the assessor** who attests that Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers has been completed. |  | | | | | |

### Protect Stored Cardholder Data

#### Requirement 3: Protect stored cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **3.1** Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific retention requirements for cardholder data * Processes for secure deletion of data when no longer needed. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.1.a** Examine the data-retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. | **Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. * Specific requirements for retention of cardholder data. * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. |  | | | | | |
| **3.1.b** Interview personnel to verify that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. | **Identify the responsible personnel** interviewed who confirm that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. |  | | | | | |
| **3.1.c** For a sample of system components that store cardholder data:   * Examine files and system records to verify that the data stored does not exceed the requirements defined in the data-retention policy. * Observe the deletion mechanism to verify data is deleted securely. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** files and system records verified that the data stored does not exceed the requirements defined in the data-retention policy. |  | | | | | |
| **Describe how** the deletion mechanism was observed to verify data is deleted securely. |  | | | | | |
| **3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.  It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:   * There is a business justification, and * The data is stored securely.   Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. | **Indicate whether** the assessed entity is an issuer or supports issuing service. **(yes/no)** |  | | | | | |
| *If “yes,” complete the responses for 3.2.a and 3.2.b and mark 3.2.c and 3.2.d as “Not Applicable.”*  *If “no,” mark the remainder of 3.2.a and 3.2.b as “Not Applicable” and proceed to 3.2.c and 3.2.d.* | | | | | | |
| **Identify** **the documentation** reviewed to verify there is a documented business justification for the storage of sensitive authentication data. |  | | | | | |
| **Identify** **the interviewed personnel** who confirm there is a documented business justification for the storage of sensitive authentication data. |  | | | | | |
| For the interview, **summarize the relevant details** of the business justification described. |  | | | | | |
| **3.2.b** For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. | *If “yes” at 3.2.a,* | | | | | | |
| **Identify** **data stores** examined. |  | | | | | |
| **Describe how** the data stores and system configurations were examined to verify that the sensitive authentication data is secured. |  | | | | | |
| **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization. | **Indicate whether** sensitive authentication data is received. **(yes/no)** |  | | | | | |
| *If “yes,” complete 3.2.c and 3.2.d.*  *If “no,” mark the remainder of 3.2.c and 3.2.d as “Not Applicable” and proceed to 3.2.1.* | | | | | | |
| **Identify** **the document(s)** reviewed to verify the data is not retained after authorization. |  | | | | | |
| **Describe how** system configurations verified that the data is not retained after authorization. |  | | | | | |
| **3.2.d** For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable. | **Identify** **the document(s)** reviewed to verify that it defines processes for securely deleting the data so that it is unrecoverable. |  | | | | | |
| **Describe how** the processes for securely deleting the data were examined to verify that the data is unrecoverable. |  | | | | | |
| **3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.  **Note:** In the normal course of business, the following data elements from the magnetic stripe may need to be retained:   * The cardholder’s name * Primary account number (PAN) * Expiration date * Service code   To minimize risk, store only these data elements as needed for business. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | **Identify the sample** of system components selected for 3.2.1-3.2.3. |  | | | | | |
| *For each data source type below from the sample of system of components examined,* **summarize the specific examples of each data source type observed** to verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | |
| * Incoming transaction data |  | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | |
| * History files |  | | | | | |
| * Trace files |  | | | | | |
| * Database schemas |  | | | | | |
| * Database contents |  | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | |
| **3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | |
| * Incoming transaction data |  | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | |
| * History files |  | | | | | |
| * Trace files |  | | | | | |
| * Database schemas |  | | | | | |
| * Database contents |  | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed**. If that type of data source is not present, indicate that in the space. | | | | | | |
| * Incoming transaction data |  | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | |
| * History files |  | | | | | |
| * Trace files |  | | | | | |
| * Database schemas |  | | | | | |
| * Database contents |  | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN.  **Note:** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.3.a** Examine written policies and procedures for masking the display of PANs to verify:   * A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. * PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. * All roles not specifically authorized to see the full PAN must only see masked PANs. | **Identify the document(s)** reviewed to verify that written policies and procedures for masking the displays of PANs include the following:   * A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. * PAN must be masked when displayed such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN. * All roles not specifically authorized to see the full PAN must only see masked PANs. |  | | | | | |
| **3.3.b** Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests. | **Describe how** system configurations verified that: | | | | | | |
| * Full PAN is only displayed for users/roles with a documented business need. |  | | | | | |
| * PAN is masked for all other requests. |  | | | | | |
| **3.3.c** Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see more than first six/last four digits of the PAN. | **Describe how** displays of PAN verified that: | | | | | | |
| * PANs are masked when displaying cardholder data. |  | | | | | |
| * Only those with a legitimate business need are able to see more than first six/last four digits of the PAN. |  | | | | | |
| **3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:   * One-way hashes based on strong cryptography, (hash must be of the entire PAN). * Truncation (hashing cannot be used to replace the truncated segment of PAN). * Index tokens and pads (pads must be securely stored). * Strong cryptography with associated key-management processes and procedures.   **Note:** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity’s environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures | **Identify** **the documentation** examined to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  | | | | | |
| **3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). | **Identify** **the sample** of data repositories selected for this testing procedure. |  | | | | | |
| **Identify** **the tables or files** examined for each item in the sample of data repositories. |  | | | | | |
| *For each item in the sample*, **describe how** the tables or files verified that the PAN is rendered unreadable. |  | | | | | |
| **3.4.c** Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable. | **Identify the sample** of removable media selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** the sample of removable media confirmed that the PAN is rendered unreadable. |  | | | | | |
| **3.4.d** Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs. | **Identify the sample** of audit logs, including payment application logs, selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** the sample of audit logs, including payment application logs, confirmed that the PAN is rendered unreadable or is not present in the logs. |  | | | | | |
| **3.4.e** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | **Identify whether** hashed and truncated versions of the same PAN are present in the environment **(yes/no)**  *If ‘no,’* mark 3.4.e as ‘not applicable’ and proceed to 3.4.1. |  | | | | | |
| *If ‘yes,’* **describe** the implemented controls examined to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. |  | | | | | |
| **3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.  *Note: This requirement applies in addition to all other PCI DSS encryption and key management requirements.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.4.1.a** If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system’s authentication mechanism (for example, not using local user account databases or general network login credentials). | **Indicate whether** disk encryption is used. **(yes/no)** |  | | | | | |
| *If “yes,” complete the remainder of 3.4.1.a, 3.4.1.b, and 3.4.1.c.*  *If “no,” mark the remainder of 3.4.1.a, 3.4.1.b and 3.4.1.c as “Not Applicable.’* | | | | | | |
| **Describe** the disk encryption mechanism(s) in use. |  | | | | | |
| *For each disk encryption mechanism in use,* **describe how** the configuration verified that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  | | | | | |
| *For each disk encryption mechanism in use*, **describe how** the authentication process was observed to verify that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  | | | | | |
| **3.4.1.b** Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls). | **Describe how** processes were observed to verify that cryptographic keys are stored securely. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that cryptographic keys are stored securely. |  | | | | | |
| **3.4.1.c** Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored.  **Note:** If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method. | **Describe how** the configurations verified that cardholder data on removable media is encrypted wherever stored. |  | | | | | |
| **Describe how** processes were observed to verify that cardholder data on removable media is encrypted wherever stored. |  | | | | | |
| **3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:  **Note:** This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. | **Identify** **the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. |  | | | | | |
| **3.5.1 *Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes:  • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date  • Description of the key usage for each key.  • Inventory of any HSMs and other SCDs used for key management  ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.1** Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including:  • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date  • Description of the key usage for each key  • Inventory of any HSMs and other SCDs used for key management | **Identify the responsible personnel interviewed** who confirm that a document exists to describe the cryptographic architecture, including:  • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date  • Description of the key usage for each key  • Inventory of any HSMs and other SCDs used for key management |  | | | | | |
| **Identify the documentation reviewed** to verify thatit contains a description of the cryptographic architecture, including:  • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date  • Description of the key usage for each key  • Inventory of any HSMs and other SCDs used for key management |  | | | | | |
| **3.5.2** Restrict access to cryptographic keys to the fewest number of custodians necessary. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.2** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary. | **Identify** **user access lists** examined. |  | | | | | |
| **Describe how** the user access lists verified that access to keys is restricted to the fewest number of custodians necessary. |  | | | | | |
| **3.5.3** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). * As at least two full-length key components or key shares, in accordance with an industry-accepted method.   **Note:** It is not required that public keys be stored in one of these forms. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.3.a** Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. | **Identify** **the documented procedures** examined to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. |  | | | | | |
| **3.5.3.b** Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one, (or more), of the following form at all times.   * Encrypted with a key-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. | **Provide the name** **of the assessor** who attests that all locations where keys are stored were identified. |  | | | | | |
| **Describe how** system configurations and key storage locations verified that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. |  | | | | | |
| **3.5.3.c** Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify:   * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. | **Describe how** system configurations and key storage locations verified that, wherever key-encrypting keys are used: | | | | | | |
| * Key-encrypting keys are at least as strong as the data-encrypting keys they protect |  | | | | | |
| * Key-encrypting keys are stored separately from data-encrypting keys. |  | | | | | |
| **3.5.4** Store cryptographic keys in the fewest possible locations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.4** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations. | **Describe how** key storage locations and the observed processes verified that keys are stored in the fewest possible locations. |  | | | | | |
| **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:  **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.a *Additional Procedure for service provider assessments only***: If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. | **Indicate whether** the assessed entity is a service provider that shares keys with their customers for transmission or storage of cardholder data. **(yes/no)** |  | | | | | |
| *If “yes,”* **Identify** **the document** that the service provider provides to their customers examined to verify that it includes guidance on how to securely transmit, store and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. |  | | | | | |
| **3.6.b** Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following: | | | | | | | |
| **3.6.1** Generation of strong cryptographic keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.1.a** Verify that key-management procedures specify how to generate strong keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to generate strong keys. |  | | | | | |
| **3.6.1.b** Observe the procedures for generating keys to verify that strong keys are generated. | **Describe how** the procedures for generating keys was observed to verify that strong keys are generated. |  | | | | | |
| **3.6.2** Secure cryptographic key distribution. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.2.a** Verify that key-management procedures specify how to securely distribute keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to securely distribute keys. |  | | | | | |
| **3.6.2.b** Observe the method for distributing keys to verify that keys are distributed securely. | **Describe how** the method for distributing keys was observed to verify that keys are distributed securely. |  | | | | | |
| **3.6.3** Secure cryptographic key storage. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.3.a** Verify that key-management procedures specify how to securely store keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to securely store keys. |  | | | | | |
| **3.6.3.b** Observe the method for storing keys to verify that keys are stored securely. | **Describe how** the method for storing keys was observed to verify that keys are stored securely. |  | | | | | |
| **3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.4.a** Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). | **Identify** **the documented key-management procedures** examined to verify procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). |  | | | | | |
| **3.6.4.b** Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s). | **Identify** the responsible **personnel interviewed** who confirm that keys are changed at the end of the defined cryptoperiod(s). |  | | | | | |
| **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.  **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.5.a** Verify that key-management procedures specify processes for the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the documented key-management procedures** examined to verify that key-management processes specify the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | |
| **3.6.5.b** Interview personnel to verify the following processes are implemented:   * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. * Keys are replaced if known or suspected to be compromised. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the responsible personnel** interviewed who confirm that the following processes are implemented:   * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. * Keys are replaced if known or suspected to be compromised. * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | |
| **3.6.6** If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.  **Note:** Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.6.a** Verify that manual clear-text key-management procedures specify processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another. | **Indicate** **whether** manual clear-text cryptographic key-management operations are used. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 3.6.6.a and 3.6.6.b as “Not Applicable.”*  *If “yes,” complete 3.6.6.a and 3.6.6.b.* | | | | | | |
| **Identify the documented key-management procedures** examined to verify that manual clear-text key-management procedures define processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials of another. |  | | | | | |
| **3.6.6.b** Interview personnel and/or observe processes to verify that manual clear-text keys are managed with:   * Split knowledge, AND * Dual control | **Identify** **the responsible personnel** interviewed for this testing procedure, if applicable. |  | | | | | |
| For the interview, **summarize the relevant details discussed and/or describe how** processeswere observed to verify that manual clear-text keys are managed with: | | | | | | |
| * Split knowledge |  | | | | | |
| * Dual Control |  | | | | | |
| **3.6.7** Prevention of unauthorized substitution of cryptographic keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.7.a** Verify that key-management procedures specify processes to prevent unauthorized substitution of keys. | **Identify** **the documented key-management procedures** examined to verify that key-management procedures specify processes to prevent unauthorized substitution of keys. |  | | | | | |
| **3.6.7.b** Interview personnel and/or observe process to verify that unauthorized substitution of keys is prevented. | **Identify** **the responsible personnel** interviewed for this testing procedure, if applicable. |  | | | | | |
| For the interview, **summarize the relevant details discussed** **and/or describe how** processes were observed to verify that unauthorized substitution of keys is prevented. |  | | | | | |
| **3.6.8** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.8.a** Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Identify** **the documented key-management procedures** examined to verify that key-management procedures specify processes for key custodians to acknowledge that they understand and accept their key-custodian responsibilities. |  | | | | | |
| **3.6.8.b** Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Describe how** key custodian acknowledgements or other evidence were observed to verify that key custodians have acknowledged that they understand and accept their key-custodian responsibilities. |  | | | | | |
| **3.7** Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.7** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are:   * Documented, * In use, and * Known to all affected parties | **Identify** **the document** reviewed to verify that security policies and operational procedures for protecting stored cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting stored cardholder data are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 4: Encrypt transmission of cardholder data across open, public networks

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:   * Only trusted keys and certificates are accepted. * The protocol in use only supports secure versions or configurations. * The encryption strength is appropriat*e* for the encryption methodology in use.   ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed**.*  *Examples of open, public networks include but are not limited to:*   * *The Internet* * *Wireless technologies, including 802.11 and Bluetooth* * *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* * *General Packet Radio Service (GPRS)* * *Satellite communications* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where cardholder data is transmitted or received over open, public networks. |  | | | | | |
| **Identify** **the documented standards** examined. |  | | | | | |
| **Describe how** the documented standards and system configurations both verified the use of: | | | | | | |
| * Security protocols for all locations |  | | | | | |
| * Strong cryptography for all locations |  | | | | | |
| **4.1.b** Review documented policies and procedures to verify processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. | **Identify the document** reviewed to verify that processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. |  | | | | | |
| **4.1.c** Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit. | **Describe** **the sample** of inbound and outbound transmissions that were observed as they occurred. |  | | | | | |
| **Describe how** the sample of inbound and outbound transmissions verified that all cardholder data is encrypted with strong cryptography during transit. |  | | | | | |
| **4.1.d** Examine keys and certificates to verify that only trusted keys and/or certificates are accepted. | *For all instances where cardholder data is transmitted or received over open, public networks:* | | | | | | |
| **Describe the mechanisms** used to ensure that only trusted keys and/or certificates are accepted. |  | | | | | |
| **Describe how** the mechanisms were observed to accept only trusted keys and/or certificates. |  | | | | | |
| **4.1.e** Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. | *For all instances where cardholder data Is transmitted or received over open, public networks,* **describe how** system configurations verified that the protocol: | | | | | | |
| * Is implemented to use only secure configurations. |  | | | | | |
| * Does not support insecure versions or configurations. |  | | | | | |
| **4.1.f** Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) | *For each encryption methodology in use,* | | | | | | |
| **Identify** vendor recommendations/best practices for encryption strength. |  | | | | | |
| **Identify** the encryption strength observed to be implemented. |  | | | | | |
| **4.1.g** For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.  *For example, for browser-based implementations:*   * *“HTTPS” appears as the browser Universal Record Locator (URL) protocol; and* * *Cardholder data is only requested if “HTTPS” appears as part of the URL.* | **Indicate whether** TLS is implemented to encrypt cardholder data over open, public networks. **(yes/no)**  *If ‘no,’ mark the remainder of 4.1.g as ‘not applicable.’* |  | | | | | |
| *If “yes,” for all instances where TLS is used to encrypt cardholder data over open, public networks,***describe how** system configurations verified that TLS is enabled whenever cardholder data is transmitted or received. |  | | | | | |
| **4.1.h** If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS. | **Indicate whether** SSL/early TLS is used. **(yes/no)**  *If ‘no,’ mark the remainder of 4.1.h as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **provide the name of the assessor** who attests that the testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS were performed. |  | | | | | |
| **4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.1** Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified:   * Industry best practices are used to implement strong encryption for authentication and transmission. * Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission. | **Identify** all wireless networks transmitting cardholder data or connected to the cardholder data environment. |  | | | | | |
| **Identify the documented standards** examined. |  | | | | | |
| **Describe how** the documented standards and system configuration settings both verified the following for all wireless networks identified: | | | | | | |
| * Industry best practices are used to implement strong encryption for authentication and transmission. |  | | | | | |
| * Weak encryption is not used as a security control for authentication or transmission. |  | | | | | |
| **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | **Indicate** **whether** end-user messaging technologies are used to send cardholder data. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 4.2.a as “Not Applicable” and proceed to 4.2.b.*  *If “yes,” complete the following:* | | | | | | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **Describe** **the sample** of outbound transmissions that were observed as they occurred. |  | | | | | |
| **Describe how** the sample of outbound transmissions verified that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **4.2.b** Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. | **Identify** **the policy document** that prohibits PAN from being sent via end-user messaging technologies under any circumstances. |  | | | | | |
| **4.3** Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.3** Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for encrypting transmissions of cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for encrypting transmissions of cardholder data are:   * In use * Known to all affected parties |  | | | | | |

### Maintain a Vulnerability Management Program

#### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  | | | | | |
| **5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | **Identify** **the vendor documentation** reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  | | | | | |
| **Describe how** anti-virus configurations verified that anti-virus programs: | | | | | | |
| * Detect all known types of malicious software, |  | | | | | |
| * Remove all known types of malicious software, and |  | | | | | |
| * Protect against all known types of malicious software. |  | | | | | |
| **5.1.2** For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.1.2** Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software. | **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, and that such systems continue to not require anti-virus software. |  | | | | | |
| **5.2** Ensure that all anti-virus mechanisms are maintained as follows:   * Are kept current. * Perform periodic scans. * Generate audit logs which are retained per PCI DSS Requirement 10.7. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.2.a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up-to-date. | **Identify** **the documented policies and procedures** examined to verify that anti-virus software and definitions are required to be kept up to date. |  | | | | | |
| **5.2.b** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are:   * Configured to perform automatic updates, and * Configured to perform periodic scans. | **Describe how** anti-virus configurations, including the master installation of the software, verified anti-virus mechanisms are: | | | | | | |
| * Configured to perform automatic updates, and |  | | | | | |
| * Configured to perform periodic scans. |  | | | | | |
| **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:   * The anti-virus software and definitions are current. * Periodic scans are performed. | **Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure. |  | | | | | |
| **Describe how** the system components verified that: | | | | | | |
| * The anti-virus software and definitions are current. |  | | | | | |
| * Periodic scans are performed. |  | | | | | |
| **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:   * Anti-virus software log generation is enabled, and * Logs are retained in accordance with PCI DSS Requirement 10.7. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, verified that: | | | | | | |
| * Anti-virus software log generation is enabled, and. |  | | | | | |
| * Logs are retained in accordance with PCI DSS Requirement 10.7. |  | | | | | |
| **5.3** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.  **Note:** Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.3.a** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software is actively running. |  | | | | | |
| **5.3.b** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users. | *For each item in the sample from 5.3.a,* **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software cannot be disabled or altered by users. |  | | | | | |
| **5.3.c** Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. | **Identify** **the responsible personnel** interviewed who confirm that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | |
| **Describe how** processes were observed to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | |
| **5.4** Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.4** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for protecting systems against malware are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting systems against malware are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 6: Develop and maintain secure systems and applications

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.  **Note:** Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.  Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.1.a** Examine policies and procedures to verify that processes are defined for the following:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. | **Identify** **the documented policies and procedures** examined to confirm that processes are defined:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. |  | | | | | |
| **6.1.b** Interview responsible personnel and observe processes to verify that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. | **Identify the responsible personnel** interviewed who confirm that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | |
| **Describe** the processes observed to verify that: | | | | | | |
| * New security vulnerabilities are identified. |  | | | | | |
| * A risk ranking is assigned to vulnerabilities to include identification of all “high” risk and “critical” vulnerabilities. |  | | | | | |
| * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | |
| **Identify** the outside sources used. |  | | | | | |
| **6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.  **Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.2.a** Examine policies and procedures related to security-patch installation to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months). | **Identify** **the documented policies and procedures** related to security-patch installation examined to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame. |  | | | | | |
| **6.2.b** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:   * That applicable critical vendor-supplied security patches are installed within one month of release. * All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). | **Identify** **the sample** of system components and related software selected for this testing procedure. |  | | | | | |
| **Identify** **the vendor security patch list** reviewed. |  | | | | | |
| *For each item in the sample,* **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify that: | | | | | | |
| * Applicable critical vendor-supplied security patches are installed within one month of release. |  | | | | | |
| * All applicable vendor-supplied security patches are installed within an appropriate time frame. |  | | | | | |
| **6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:   * In accordance with PCI DSS (for example, secure authentication and logging). * Based on industry standards and/or best practices. * Incorporate information security throughout the software development life cycle.   **Note**: this applies to all software developed internally as well as bespoke or custom software developed by a third party. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.3.a** Examine written software-development processes to verify that the processes are based on industry standards and/or best practices. | **Identify** **the document** examined to verify that software-development processes are based on industry standards and/or best practices. |  | | | | | |
| **6.3.b** Examine written software development processes to verify that information security is included throughout the life cycle. | **Identify** **the documented software development processes** examined to verify that information security is included throughout the life cycle. |  | | | | | |
| **6.3.c** Examine written software development processes to verify that software applications are developed in accordance with PCI DSS. | **Identify** **the documented software development processes** examined to verify that software applications are developed in accordance with PCI DSS. |  | | | | | |
| **6.3.d** Interview software developers to verify that written software development processes are implemented. | **Identify** **the software developers** interviewed who confirm that written software development processes are implemented. |  | | | | | |
| **6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.3.1** Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. | **Identify** **the documented software-development processes** examined to verify processes define that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | |
| **6.3.2** Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:   * Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines. * Appropriate corrections are implemented prior to release. * Code review results are reviewed and approved by management prior to release.   **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.  *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.3.2.a** Examine written software development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. | **Identify** **the documented software-development processes** examined to verify processes define that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | |
| **6.3.2.b** Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above. | **Identify** **the sample** of recent custom application changes selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** code review processes were observed to verify custom application code is reviewed as follows: | | | | | | |
| * Code changes are reviewed by individuals other than the originating code author. |  | | | | | |
| * Code changes are reviewed by individuals who are knowledgeable in code-review techniques and secure coding practices. |  | | | | | |
| * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). |  | | | | | |
| * Appropriate corrections are implemented prior to release. |  | | | | | |
| * Code-review results are reviewed and approved by management prior to release. |  | | | | | |
| **6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4** Examine policies and procedures to verify the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change control procedures related to implementing security patches and software modifications are documented. | **Identify the documented policies and procedures** examined to verify that the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change-control procedures related to implementing security patches and software modifications are documented. |  | | | | | |
| **6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.1.a** Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s). | **Identify the network documentation** examined to verify that the development/test environments are separate from the production environment(s). |  | | | | | |
| **Describe how** network device configurations verified that the development/test environments are separate from the production environment(s). |  | | | | | |
| **6.4.1.b** Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s). | **Identify the access control settings** examined for this testing procedure. |  | | | | | |
| **Describe how** the access control settings verified that access controls are in place to enforce separation between the development/test environments and the production environment(s). |  | | | | | |
| **6.4.2** Separation of duties between development/test and production environments. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.2** Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment. | **Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | |
| **Identify the personnel assigned to production environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | |
| **Describe how** processes were observed to verify that separation of duties is in place between development/test environments and the production environment. |  | | | | | |
| **6.4.3** Production data (live PANs) are not used for testing or development. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development. | **Identify the responsible personnel** interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development. |  | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing. |  | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development. |  | | | | | |
| **6.4.3.b** Examine a sample of test data to verify production data (live PANs) is not used for testing or development. | **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for testing. |  | | | | | |
| **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for development. |  | | | | | |
| **6.4.4** Removal of test data and accounts from system components before the system becomes active / goes into production. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.4.a** Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active. | **Identify the responsible personnel** interviewed who confirm that test data and accounts are removed before a production system becomes active. |  | | | | | |
| **Describe how** testing processes were observed to verify that test data is removed before a production system becomes active. |  | | | | | |
| **Describe how** testing processes were observed to verify that test accounts are removed before a production system becomes active. |  | | | | | |
| **6.4.4.b** Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active. | **Describe how** the sampled data examined verified that test data is removed before the system becomes active. |  | | | | | |
| **Describe how** the sampled data examined verified that test accounts are removed before the system becomes active. |  | | | | | |
| **6.4.5** Change control procedures must include the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.a** Examine documented change-control procedures and verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. | **Identify** **the documented change-control procedures** examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  | | | | | |
| **6.4.5.b** For a sample of system components, interview responsible personnel to determine recent changes. Trace those changes back to related change control documentation. For each change examined, perform the following: | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| **Identify the responsible personnel** interviewed to determine recent changes. |  | | | | | |
| *For each item in the sample,* **identify** **the sample** of changes and the related change control documentation selected for this testing procedure (through 6.4.5.4). |  | | | | | |
| **6.4.5.1** Documentation of impact. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change. | *For each change from 6.4.5.b*, **describe how** the documentation of impact is included in the change control documentation for each sampled change. |  | | | | | |
| **6.4.5.2** Documented change approval by authorized parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change. | *For each change from 6.4.5.b*, **describe how** documented approval by authorized parties is present in the change control documentation for each sampled change. |  | | | | | |
| **6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. | *For each change from 6.4.5.b*, **describe how** the change control documentation confirmed that functionality testing is performed to verify that the change does not adversely impact the security of the system. |  | | | | | |
| **6.4.5.3.b** For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **identify** **the sample** of custom code changes and the related change control documentation selected for this testing procedure. |  | | | | | |
| For each change, **describe how** the change control documentation verified that updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. |  | | | | | |
| **6.4.5.4** Back-out procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.4** Verify that back-out procedures are prepared for each sampled change. | *For each change from 6.4.5.b*, **describe how** the change control documentation verified that back-out procedures are prepared. |  | | | | | |
| **6.4.6** Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.  ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.6** For a sample of significant changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change. | **Identify whether** a significant change occurred within the past 12 months. **(yes/no)**  *If “yes,” complete the following:*  *If “no,” mark the rest of 6.4.6 as “Not Applicable”* |  | | | | | |
| **Identify the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| **Identify the relevant documentation** reviewed to verify that the documentation was updated as part of the change. |  | | | | | |
| **Identify the sample of change records** examined for this testing procedure. |  | | | | | |
| **Identify the sample of systems/networks** affected by the significant change. |  | | | | | |
| *For each sampled change,* **describe how**the system/networks observed verified that applicable PCI DSS requirements were implemented and documentation updated as part of the change. | | | | | | |
|  | | | | | | |
| **6.5** Address common coding vulnerabilities in software-development processes as follows:   * Traindevelopers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. * Develop applications based on secure coding guidelines.   **Note:** The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.a** Examine software development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers at least annually, based on industry best practices and guidance. | **Identify** **the document** reviewed to verify that up-to-date training in secure coding techniques is required for developers at least annually. |  | | | | | |
| **Identify** the industry best practices and guidance on which the training is based. |  | | | | | |
| **6.5.b** Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities | **Identify the records** **of training** that were examined to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities. |  | | | | | |
| **6.5.c** Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: | **Identify** **the software-development policies and procedures** examined to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10. |  | | | | | |
| **Identify** **the responsible personnel** interviewed to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10. |  | | | | | |
| **Note:** Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external): | | | | | | | |
| **6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.1** Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include:   * Validating input to verify user data cannot modify meaning of commands and queries. * Utilizing parameterized queries. | *For the interviews at 6.5.d***, summarize the relevant details** discussed to verify that injection flaws are addressed by coding techniques that include: | | | | | | |
| * Validating input to verify user data cannot modify meaning of commands and queries. |  | | | | | |
| * Utilizing parameterized queries. |  | | | | | |
| **6.5.2** Buffer overflow. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.2** Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include:   * Validating buffer boundaries. * Truncating input strings. | *For the interviews at 6.5.d***, summarize the relevant details** discussed to verify that buffer overflows are addressed by coding techniques that include: | | | | | | |
| * Validating buffer boundaries. |  | | | | | |
| * Truncating input strings. |  | | | | | |
| **6.5.3** Insecure cryptographic storage. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.3** Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that:   * Prevent cryptographic flaws. * Use strong cryptographic algorithms and keys. | *For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that insecure cryptographic storage is addressed by coding techniques that: | | | | | | |
| * Prevent cryptographic flaws. |  | | | | | |
| * Use strong cryptographic algorithms and keys. |  | | | | | |
| **6.5.4** Insecure communications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.4** Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications. | *For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that insecure communications are addressed by coding techniques that properly: | | | | | | |
| * Authenticate all sensitive communications. |  | | | | | |
| * Encrypt all sensitive communications. |  | | | | | |
| **6.5.5** Improper error handling. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.5** Examine-software development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages(for example, by returning generic rather than specific error details). | *For the interviews at 6.5.d***, summarize the relevant details** discussed to verify that improper error handling is addressed by coding techniques that do not leak information via error messages. |  | | | | | |
| **6.5.6** All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.6** Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1. | *For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1. |  | | | | | |
| **Note:** Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external): | | | | | | | |
| **Indicate** **whether** web applications and application interfaces are present. **(yes/no)**  *If “no,”* mark the below 6.5.7-6.5.10 as “Not Applicable.”  *If “yes,”* ***complete the following:*** | |  | | | | | |
| **6.5.7** Cross-site scripting (XSS). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.7** Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include:   * Validating all parameters before inclusion. * Utilizing context-sensitive escaping. | *For the interviews at 6.5.d***, summarize the relevant details** discussed to verify that cross-site scripting (XSS) is addressed by coding techniques that include: | | | | | | |
| * Validating all parameters before inclusion. |  | | | | | |
| * Utilizing context-sensitive escaping. |  | | | | | |
| **6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.8** Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that include:   * Proper authentication of users. * Sanitizing input. * Not exposing internal object references to users. * User interfaces that do not permit access to unauthorized functions. | *For the interviews at 6.5.d***, summarize the relevant details** discussed to verify that improper access control is addressed by coding techniques that include: | | | | | | |
| * Proper authentication of users. |  | | | | | |
| * Sanitizing input. |  | | | | | |
| * Not exposing internal object references to users. |  | | | | | |
| * User interfaces that do not permit access to unauthorized functions. |  | | | | | |
| **6.5.9** Cross-site request forgery (CSRF). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.9** Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. | *For the interviews at 6.5.d***, summarize the relevant details** discussed to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. |  | | | | | |
| **6.5.10** Broken authentication and session management**.** | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.10** Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include:   * Flagging session tokens (for example cookies) as “secure.” * Not exposing session IDs in the URL. * Incorporating appropriate time-outs and rotation of session IDs after a successful login. | *For the interviews at 6.5.d,* **summarize the relevant details** discussed to verify that broken authentication and session management are addressed via coding techniques that commonly include: | | | | | | |
| * Flagging session tokens (for example cookies) as “secure.” |  | | | | | |
| * Not exposing session IDs in the URL. |  | | | | | |
| * Incorporating appropriate time-outs and rotation of session IDs after a successful login. |  | | | | | |
| **6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:   * Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.   **Note:** This assessment is not the same as the vulnerability scans performed for Requirement 11.2.   * Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.6** For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows:   * Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. * Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. | For each public-facing web application, **identify which** of the two methods are implemented:   * Web application vulnerability security assessments, AND/OR * Automated technical solution that detects and prevents web-based attacks, such as web application firewalls. |  | | | | | |
| *If application vulnerability security assessments are indicated above:* | | | | | | |
| **Describe the tools and/or methods** used (manual or automated, or a combination of both). |  | | | | | |
| **Identify the documented processes** that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected * That the application is re-evaluated after the corrections. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that public-facing web applications are reviewed, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. |  | | | | | |
| **Identify the records of application vulnerability security assessments** examined for this testing procedure. |  | | | | | |
| **Describe how** the records of application vulnerability security assessments verified that public-facing web applications are reviewed as follows: | | | | | | |
| * At least annually. |  | | | | | |
| * After any changes. |  | | | | | |
| * By an organization that specialized in application security. |  | | | | | |
| * That at a minimum, all vulnerabilities in requirement 6.5 are included in the assessment. |  | | | | | |
| * That all vulnerabilities are corrected. |  | | | | | |
| * That the application is re-evaluated after the corrections. |  | | | | | |
| *If an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is indicated above:* | | | | | | |
| **Describe** the automated technical solution in use that detects and prevents web-based attacks. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above automated technical solution is in place as follows:   * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | |
| **Describe how** the system configuration settings verified that the above automated technical solution is in place as follows: | | | | | | |
| * Is situated in front of public-facing web applications to detect and prevent web-based attacks. |  | | | | | |
| * Is actively running and up-to-date as applicable. |  | | | | | |
| * Is generating audit logs. |  | | | | | |
| * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | |
| **6.7** Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.7** Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** examined to verify that security policies and operational procedures for developing and maintaining secure systems and applications are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for developing and maintaining secure systems and applications are:   * In use * Known to all affected parties |  | | | | | |

### Implement Strong Access Control Measures

#### Requirement 7: Restrict access to cardholder data by business need to know

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.a** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function. * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  | | | | | |
| **7.1.1** Define access needs for each role, including:   * System components and data resources that each role needs to access for their job function. * Level of privilege required (for example, user, administrator, etc.) for accessing resources. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.1** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | **Identify** **the selected sample** of roles for this testing procedure. |  | | | | | |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs are defined and include: | | | | | | |
| * System components and data resources that each role needs to access for their job function. |  | | | | | |
| * Identification of privilege necessary for each role to perform their job function. |  | | | | | |
| **7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.2.a** Interview personnel responsible for assigning access to verify that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.2.b** Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the sample** of user IDs ***with privileged access*** selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed to confirm that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are: | | | | | | |
| * Necessary for that individual’s job function. |  | | | | | |
| * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.3** Assign access based on individual personnel’s job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.3** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. | **Identify the sample** of user IDs selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed who confirm that privileges assigned are based on that individual’s job classification and function. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are based on that individual’s job classification and function. |  | | | | | |
| **7.1.4** Require documented approval by authorized parties specifying required privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.4** Select a sample of user IDs and compare with documented approvals to verify that:   * Documented approval exists for the assigned privileges. * The approval was by authorized parties. * That specified privileges match the roles assigned to the individual. | **Identify the sample** of user IDs selected for this testing procedure. |  | | | | | |
| For each user ID in the selected sample, **describe how**: | | | | | | |
| * Documented approval exists for the assigned privileges. |  | | | | | |
| * The approval was by authorized parties. |  | | | | | |
| * That specified privileges match the roles assigned to the individual. |  | | | | | |
| **7.2** Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.  This access control system(s) must include the following: | | | | | | | |
| **7.2** Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows: | | | | | | | |
| **7.2.1** Coverage of all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.1** Confirm that access control systems are in place on all system components. | **Identify** **vendor documentation** examined. |  | | | | | |
| **Describe how** system settings and the vendor documentation verified that access control systems are in place on all system components. |  | | | | | |
| **7.2.2** Assignment of privileges to individuals based on job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | **Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  | | | | | |
| **7.2.3** Default “deny-all” setting. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.3** Confirm that the access control systems have a default “deny-all” setting. | **Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems have a default “deny-all” setting. |  | | | | | |
| **7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.3** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting access to cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for restricting access to cardholder data are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 8: Identify and authenticate access to system components

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.a** Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8:   * Assign all users a unique ID before allowing them to access system components or cardholder data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  | | | | | |
| **8.1.b** Verify that procedures are implemented for user identification management, by performing the following: | | | | | | | |
| **8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.1** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data. | **Identify** **the responsible administrative personnel** interviewed who confirm that all users are assigned a unique ID for access to system components or cardholder data. |  | | | | | |
| **8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.2** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval. | **Identify** **the sample** of privileged user IDs selected for this testing procedure. |  | | | | | |
| **Identify** **the sample** of general user IDs selected for this testing procedure. |  | | | | | |
| **Describe how** observed system settings and the associated authorizations verified that each ID has been implemented with only the privileges specified on the documented approval: | | | | | | |
| * For the sample of privileged user IDs. |  | | | | | |
| * For the sample of general user IDs. |  | | | | | |
| **8.1.3** Immediately revoke access for any terminated users. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.3.a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** **the sample** of users terminated in the past six months that were selected for this testing procedure. |  | | | | | |
| **Describe how** the current user access lists for ***local access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **Describe how** the current user access lists for ***remote access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **8.1.3.b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  | | | | | |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  | | | | | |
| **8.1.4** Remove/disable inactive user accounts within 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. | **Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled. |  | | | | | |
| **8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:   * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.5.a** Interview personnel and observe processes for managing accounts used by third parties to access, support, or maintain system components to verify that accounts used for remote access are:   * Disabled when not in use. * Enabled only when needed by the third party, and disabled when not in use. | **Identify** **the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are:   * Disabled when not in use. * Enabled only when needed by the third party, and disabled when not in use. |  | | | | | |
| **Describe how** processes for managing third party accounts were observed to verify that accounts used for remote access are: | | | | | | |
| * Disabled when not in use. |  | | | | | |
| * Enabled only when needed by the third party, and disabled when not in use. |  | | | | | |
| **8.1.5.b** Interview personnel and observe processes to verify that third party remote access accounts are monitored while being used. | **Identify** **the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are monitored while being used. |  | | | | | |
| **Describe how** processes for managing third party remote access were observed to verify that accounts are monitored while being used. |  | | | | | |
| **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that authentication parameters are set to require that user accounts be locked after not more than six invalid logon attempts. |  | | | | | |
| **8.1.6.b** ***Additional procedure for service provider assessments only:*** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **Describe how** implemented processes were observed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. |  | | | | | |
| **8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that system/session idle time out features have been set to 15 minutes or less. |  | | | | | |
| **8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:   * Something you know, such as a password or passphrase. * Something you have, such as a token device or smart card. * Something you are, such as a biometric. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following:   * Examine documentation describing the authentication method(s) used. * For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s). | **Identify the document** describing the authentication method(s) used that was reviewed to verify that the methods require users to be authenticated using a unique ID and additional authentication for access to the cardholder data environment. |  | | | | | |
| **Describe** the authentication methods used (for example, a password or passphrase, a token device or smart card, a biometric, etc.) for each type of system component. |  | | | | | |
| *For each type of authentication method used and for each type of system component,* **describe how** the authentication method was observed to be functioning consistently with the documented authentication method(s). |  | | | | | |
| **8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.1.a** Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage. | **Identify** **the vendor documentation** examined to verify that passwords are protected with strong cryptography during transmission and storage. |  | | | | | |
| **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,***describe how** system configuration settings verified that passwords are protected with strong cryptography during ***transmission***. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that passwords are protected with strong cryptography during ***storage***. |  | | | | | |
| **8.2.1.b** For a sample of system components, examine password files to verify that passwords are unreadable during storage. | *For each item in the sample at 8.2.1.a,* **describe how** password files verified that passwords are unreadable during storage. |  | | | | | |
| **8.2.1.c** For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission. | *For each item in the sample at 8.2.1.a,* **describe how** password files verified that passwords are unreadable during transmission. |  | | | | | |
| **8.2.1.d** ***Additional procedure for service provider assessments only:*** Observe password files to verify that non-consumer customer passwords are unreadable during storage. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during storage. |  | | | | | |
| **8.2.1.e *Additional procedure for service provider assessments only:*** Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during transmission. |  | | | | | |
| **8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.2** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. | **Identify the document** examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  | | | | | |
| **Describe** the non-face-to-face methods used for requesting password resets. |  | | | | | |
| For each non-face-to-face method, **describe how** security personnel were observed to verify the user’s identity before the authentication credential was modified. |  | | | | | |
| **8.2.3** Passwords/passphrases must meet the following:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters.   Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.3.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that user password/passphrase parameters are set to require at least the following strength/complexity: | | | | | | |
| * Require a minimum length of at least seven characters. |  | | | | | |
| * Contain both numeric and alphabetic characters. |  | | | | | |
| **8.2.3.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | *Additional procedure for service provider assessments only:***Identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:   * A minimum length of at least seven characters. * Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters. |  | | | | | |
| **Describe how** internal processes were observed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: | | | | | | |
| * A minimum length of at least seven characters. |  | | | | | |
| * Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters. |  | | | | | |
| **8.2.4** Change user passwords/passphrases at least once every 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days. |  | | | | | |
| **8.2.4.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that:   * Non-consumer customer user passwords/passphrases are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that:   * Non-consumer customer user passwords/passphrases are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. |  | | | | | |
| **Describe how** internal processes were observed to verify that: | | | | | | |
| * Non-consumer customer user passwords/passphrases are required to change periodically; and |  | | | | | |
| * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. |  | | | | | |
| **8.2.5** Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password/passphrases parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that password/passphrase parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. |  | | | | | |
| **8.2.5.b** ***Additional Procedure for service provider assessments only:*** Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. |  | | | | | |
| **Describe how** internal processes were observed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. |  | | | | | |
| **8.2.6** Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use. | **Identify** **the documented password procedures** examined to verify the procedures define that:   * First-time passwords/passphrases must be set to a unique value for each user. * First-time passwords/passphrases must be changed after the first use. * Reset passwords/passphrases must be set to a unique value for each user. * Reset passwords/passphrases must be changed after the first use. |  | | | | | |
| **Describe how** security personnel were observed to: | | | | | | |
| * Set first-time passwords/passphrases to a unique value for each new user. |  | | | | | |
| * Set first-time passwords/passphrases to be changed after first use. |  | | | | | |
| * Set reset passwords/passphrases to a unique value for each existing user. |  | | | | | |
| * Set reset passwords/passphrases to be changed after first use. |  | | | | | |
| **8.3** Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication  **Note:** Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. | | | | | | | |
| **8.3.1** Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.  ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.1.a** Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE. | **Identify the sample of network and/or system components** examined for this testing procedure. |  | | | | | |
| **Describe how** the configurations verify that multi-factor authentication is required for all non-console access into the CDE. | | | | | | |
|  | | | | | | |
| **8.3.1.b** Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used. | **Identify the sample of administrator personnel** observed logging in to the CDE. |  | | | | | |
| **Describe** the multi-factor authentication methods observed to be in place for a personnel non-console log ins to the CDE. | | | | | | |
|  | | | | | | |
| **8.3.2** Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity’s network. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.2.a** Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for:   * All remote access by personnel, both user and administrator, and * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). | **Describe how** system configurations for remote access servers and systems verified that multi-factor authentication is required for: | | | | | | |
| * All remote access by personnel, both user and administrator, and |  | | | | | |
| * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). |  | | | | | |
| **8.3.2.b** Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used. | **Identify the sample of personnel** observed connecting remotely to the network. |  | | | | | |
| *For each individual in the sample,* **describe how** multi-factor authentication was observed to be required for remote access to the network. |  | | | | | |
| **8.4** Document and communicate authentication policies and procedures to all users including:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.4.a** Examineprocedures and interview personnel to verify that authentication policies and procedures are distributed to all users. | **Identify** **the documented policies and procedures** examined to verify authentication procedures define that authentication procedures and policies are distributed to all users. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that authentication policies and procedures are distributed to all users. |  | | | | | |
| **8.4.b** Review authentication policies and procedures that are distributed to users and verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | **Identify the documented authentication policies and procedures that** **are distributed to users** reviewed to verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * That users should change passwords if there is any suspicion the password could be compromised. |  | | | | | |
| **8.4.c** Interview a sample of users to verify that they are familiar with authentication policies and procedures. | **Identify** **the sample** of users interviewed for this testing procedure. |  | | | | | |
| For each user in the sample, **summarize the relevant details** discussed that verify that they are familiar with authentication policies and procedures. |  | | | | | |
| **8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:   * Generic user IDs are disabled or removed. * Shared user IDs do not exist for system administration and other critical functions. * Shared and generic user IDs are not used to administer any system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.a** For a sample of system components, examine user ID lists to verify the following:   * Generic user IDs are disabled or removed. * Shared user IDs for system administration activities and other critical functions do not exist. * Shared and generic user IDs are not used to administer any system components. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** the user ID lists verified that: | | | | | | |
| * Generic user IDs are disabled or removed. |  | | | | | |
| * Shared user IDs for system administration activities and other critical functions do not exist. |  | | | | | |
| * Shared and generic user IDs are not used to administer any system components. |  | | | | | |
| **8.5.b** Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. | **Identify** **the documented policies and procedures** examined to verify authentication policies/procedures define that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. |  | | | | | |
| **8.5.c** Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. | **Identify** **the system administrators** interviewed who confirm that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. |  | | | | | |
| **8.5.1** ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.  This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.1** ***Additional procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer. | **Identify** **the documented procedures** examined to verify that different authentication credentials are used for access to each customer. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that different authentication credentials are used for access to each customer |  | | | | | |
| **8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows:   * Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.6.a** Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. | **Identify** **the documented authentication policies and procedures** examined to verify the procedures for using authentication mechanisms define that:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.6.b** Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts. | **Identify the security personnel** interviewed who confirm that authentication mechanisms are assigned to an account and not shared among multiple accounts. |  | | | | | |
| **8.6.c** Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings and/or physical controls, as applicable, verified that controls are implemented to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:   * All user access to, user queries of, and user actions on databases are through programmatic methods. * Only database administrators have the ability to directly access or query databases. * Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.7.a** Review database and application configuration settings and verify that all users are authenticated prior to access. | **Identify** all databases containing cardholder data. |  | | | | | |
| **Describe how** database and/or application configuration settings verified that all users are authenticated prior to access. |  | | | | | |
| **8.7.b** Examine database and application configuration settings to verify thatall user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). | *For each database from 8.7.a,* **describe how** the database and application configuration settings verified that all user access to, user queries of, and user actions on the database are through programmatic methods only. |  | | | | | |
| **8.7.c** Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators. | *For each database from 8.7.a*, **describe how** database application configuration settings verified that user direct access to or queries of databases are restricted to database administrators. |  | | | | | |
| **8.7.d** Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes). | *For each database from 8.7.a:* | | | | | | |
| * **Identify** applications with access to the database. |  | | | | | |
| * **Describe how** database access control settings, database application configuration settings and related application IDs verified that application IDs can only be used by the applications. |  | | | | | |
| **8.8** Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.8** Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for identification and authentication are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for identification and authentication are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 9: Restrict physical access to cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. * Observe a system administrator’s attempt to log into consoles for randomly selected systems in the cardholder data environment and verify that they are “locked” to prevent unauthorized use. | **Identify and briefly describe** all of the following with systems in the cardholder data environment: | | | | | | |
| * All computer rooms |  | | | | | |
| * All data centers |  | | | | | |
| * Any other physical areas |  | | | | | |
| *For each area identified (add rows as needed),* complete the following: | | | | | | |
| **Describe** the physical security controls observed to be in place, including authorized badges and lock and key. |  | | | | | |
| **Identify** the randomly selected systems in the cardholder environment for which a system administrator login attempt was observed. |  | | | | | |
| **Describe how** consoles for the randomly selected systems were observed to be “locked” when not in use. |  | | | | | |
| **9.1.1** Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.  **Note:** “Sensitive areas” refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1.1.a** Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas. | **Describe** either the video cameras or access control mechanisms (or both) observed to monitor the entry/exit points to sensitive areas. |  | | | | | |
| **9.1.1.b** Verify that either video cameras or access control mechanisms (or both) are protected from tampering or disabling. | **Describe how** either the video cameras or access control mechanisms (or both) were observed to be protected from tampering and/or disabling. |  | | | | | |
| **9.1.1.c** Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months. | **Describe how** the data from video cameras and/or access control mechanisms were observed to be reviewed. |  | | | | | |
| **Describe how** data was observed to be stored for at least three months. |  | | | | | |
| **9.1.2** Implement physical and/or logical controls to restrict access to publicly accessible network jacks.  For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly-accessible network jacks. | **Identify the responsible personnel** interviewed who confirm that physical and/or logical controls are in place to restrict access to publicly accessible network jacks. |  | | | | | |
| **Describe how** physical and/or logical controls were observed to be in place to restrict access to publicly-accessible network jacks. |  | | | | | |
| **9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted. | **Describe how** physical access was observed to be restricted to the following: | | | | | | |
| * Wireless access points |  | | | | | |
| * Wireless gateways |  | | | | | |
| * Wireless handheld devices |  | | | | | |
| * Network/communications hardware |  | | | | | |
| * Telecommunication lines |  | | | | | |
| **9.2** Develop procedures to easily distinguish between onsite personnel and visitors, to include:   * Identifying onsite personnel and visitors (for example, assigning badges). * Changes to access requirements. * Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.2.a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | **Identify** **the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  | | | | | |
| **9.2.b** Examine identification methods (such as ID badges) andobserve processes for identifying and distinguishing between onsite personnel and visitors to verify that:   * Visitors are clearly identified, and * It is easy to distinguish between onsite personnel and visitors. | **Identify** the identification methods examined. |  | | | | | |
| **Describe how** processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that: | | | | | | |
| * Visitors are clearly identified, and |  | | | | | |
| * It is easy to distinguish between onsite personnel and visitors. |  | | | | | |
| **9.2.c** Verify that access to the identification process (such as a badge system) is limited to authorized personnel. | **Describe how** access to the identification process was observed to be limited to authorized personnel. |  | | | | | |
| **9.3** Control physical access for onsite personnel to sensitive areas as follows:   * Access must be authorized and based on individual job function. * Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.3.a** For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that:   * Access to the sensitive area is authorized. * Access is required for the individual’s job function. | **Identify the sample** of onsite personnel with physical access to sensitive areas that were interviewed for this testing procedure. |  | | | | | |
| *For the interview,* **summarize the relevant details** discussed to verify that: | | | | | | |
| * Access to the sensitive area is authorized. |  | | | | | |
| * Access is required for the individual’s job function. |  | | | | | |
| **9.3.b** Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access. | **Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access. |  | | | | | |
| **9.3.c** Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas. | **Identify** **the sample** of users recently terminated. |  | | | | | |
| *For all items in the sample,* **provide the name of the assessor** who attests that the access control lists were reviewed to verify the personnel do not have physical access to sensitive areas. |  | | | | | |
| **9.4** Implement procedures to identify and authorize visitors.  Procedures should include the following: | | | | | | | |
| **9.4** Verify that visitor authorization and access controls are in place as follows: | | | | | | | |
| **9.4.1** Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.1.a** Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. | **Identify the documented procedures** examined to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.: |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. |  | | | | | |
| **9.4.1.b** Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. | **Describe how** the use of visitor badges or other identification was observed to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. |  | | | | | |
| **9.4.2** Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.2.a** Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel. | **Describe how** people within the facility were observed to use visitor badges or other identification. |  | | | | | |
| **Describe how** visitors within the facility were observed to be easily distinguishable from onsite personnel. |  | | | | | |
| **9.4.2.b** Verify that visitor badges or other identification expire. | **Describe how** visitor badges or other identification were verified to expire. |  | | | | | |
| **9.4.3** Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.3** Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration. | **Describe how** visitors leaving the facility were observed to verify they are asked to surrender their badge or other identification upon departure or expiration. |  | | | | | |
| **9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.  Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log.  Retain this log for a minimum of three months, unless otherwise restricted by law. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.4.a** Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. | **Describe how** it was observed that a visitor log is in use to record physical access to: | | | | | | |
| * The facility. |  | | | | | |
| * Computer rooms and data centers where cardholder data is stored or transmitted. |  | | | | | |
| **9.4.4.b** Verify that the log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. | **Provide the name of the assessor** who attests that the visitor log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. |  | | | | | |
| **9.4.4.c** Verify that the log is retained for at least three months. | **Describe how** visitor logs were observed to be retained for at least three months. |  | | | | | |
| **9.5** Physically secure all media. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.5** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). | **Identify the documented procedures for protecting cardholder data** reviewed to verify controls for physically securing all media are defined. |  | | | | | |
| **9.5.1** Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.5.1** Verify that the storage location security is reviewed at least annually to confirm that backup media storage is secure. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  | | | | | |
| **9.6** Maintain strict control over the internal or external distribution of any kind of media, including the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  | | | | | |
| **9.6.1** Classify media so the sensitivity of the data can be determined. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6.1** Verify that all media is classified so the sensitivity of the data can be determined. | **Describe how** media was observed to be classified so the sensitivity of the data can be determined. |  | | | | | |
| **9.6.2** Send the media by secured courier or other delivery method that can be accurately tracked. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6.2.a** Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. | **Identify** **the responsible personnel** interviewed who confirm that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. |  | | | | | |
| **Identify the records** examined for this testing procedure. |  | | | | | |
| **Describe how** the offsite tracking records verified that all media is logged and sent via secured courier or other delivery method that can be tracked. |  | | | | | |
| **9.6.2.b** Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented. | **Identify the sample** of recent offsite tracking logs for all media selected. |  | | | | | |
| *For each item in the sample,* **describe how** tracking details were observed to be documented. |  | | | | | |
| **9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6.3** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | **Identify** **the** **responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  | | | | | |
| *For each item in the sample in 9.6.2.b,* **describe how** proper management authorization was observed to be obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  | | | | | |
| **9.7** Maintain strict control over the storage and accessibility of media. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.7** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. | **Identify the documented policy** **for controlling storage and maintenance of all media** that was reviewed to verify that the policy defines required periodic media inventories. |  | | | | | |
| **9.7.1** Properly maintain inventory logs of all media and conduct media inventories at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.7.1** Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually. | **Identify the media inventories logs** reviewed. |  | | | | | |
| **Describe how** the media inventory logs verified that: | | | | | | |
| * Media inventory logs of all media were observed to be maintained. |  | | | | | |
| * Media inventories are performed at least annually. |  | | | | | |
| **9.8** Destroy media when it is no longer needed for business or legal reasons as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.8** Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). |  | | | | | |
| **9.8.1** Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.8.1.a** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | **Identify** **the responsible personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  | | | | | |
| **Provide the name of the assessor** who attests that the procedures state that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. |  | | | | | |
| **9.8.1.b** Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured. | **Describe how** the storage containers used for materials to be destroyed were verified to be secured. |  | | | | | |
| **9.8.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.8.2** Verify that cardholder data on electronic media is rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. |  | | | | | |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify the industry-accepted standards** used. |  | | | | | |
| **9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.  **Note:** These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9** Examine documented policies and procedures to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. | **Identify the documented policies and procedures** examined to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. |  | | | | | |
| **9.9.1** Maintain an up-to-date list of devices. The list should include the following:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9.1.a** Examine the list of devices to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | **Identify the documented up-to-date list of devices** examined to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. |  | | | | | |
| **9.9.1.b** Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date. | **Identify the sample** of devices from the list selected for this testing procedure. |  | | | | | |
| *For all items in the sample,* **describe how** the devices and device locations were observed to verify that the list is accurate and up-to-date. |  | | | | | |
| **9.9.1.c** Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc. | **Identify the responsible personnel** interviewed who confirm the list of devices is updated when devices are added, relocated, decommissioned, etc. |  | | | | | |
| **9.9.2** Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).  **Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9.2.a** Examine documented procedures to verify processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. |  | | | | | | |
| **Identify** **the documented procedures** examined to verify that processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. |  | | | | | |
| **9.9.2.b** Interview responsible personnel and observe inspection processes to verify:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. | **Identify** the **responsible personnel** interviewed who confirm that:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. |  | | | | | |
| **Describe how** inspection processes were observed to verify that: | | | | | | |
| * All devices are periodically inspected for evidence of tampering. |  | | | | | |
| * All devices are periodically inspected for evidence of substitution. |  | | | | | |
| **9.9.3** Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:   * Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Do not install, replace, or return devices without verification. * Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9.3.a** Review training materials for personnel at point-of-sale locations to verify it includes training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | **Identify** **the training materials for personnel at point-of-sale locations** that were reviewed to verify the materials include training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting all suspicious behavior to appropriate personnel (for example, a manager or security officer). * Reporting tampering or substitution of devices. |  | | | | | |
| **9.9.3.b** Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | **Identify** **the sample** of personnel at point-of-sale locations interviewed. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify interviewees have received training and are aware of the procedures for the following: | | | | | | |
| * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. |  | | | | | |
| * Not to install, replace, or return devices without verification. |  | | | | | |
| * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). |  | | | | | |
| * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). |  | | | | | |
| **9.10** Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.10** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting physical access to cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for restricting physical access to cardholder data are: | | | | | | |
| * In use |  | | | | | |
| * Known to all affected parties |  | | | | | |

### Regularly Monitor and Test Networks

#### Requirement 10: Track and monitor all access to network resources and cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **10.1** Implement audit trails to link all access to system components to each individual user. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.1** Verify, through observation and interviewing the system administrator, that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. | **Identify the system administrator(s)** interviewed who confirm that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. |  | | | | | |
| **Describe how** audit trails were observed to verify the following: | | | | | | |
| * Audit trails are enabled and active for system components. |  | | | | | |
| * Access to system components is linked to individual users. |  | | | | | |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following: | **Identify the responsible personnel** interviewed who confirm the following from 10.2.1-10.2.7 are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  | | | | | |
| **Identify the sample of audit logs** selected for 10.2.1-10.2.7. |  | | | | | |
| **10.2.1** All individual user accesses to cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1** Verify all individual access to cardholder data is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings verified that all individual access to cardholder data is logged. |  | | | | | |
| **10.2.2** All actions taken by any individual with root or administrative privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.2** Verify all actions taken by any individual with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings verifiedall actions taken by any individual with root or administrative privileges are logged. |  | | | | | |
| **10.2.3** Access to all audit trails. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.3** Verify access to all audit trails is logged. | *For all items in the sample at 10.2*, **describe how** configuration settings verified that access to all audit trails is logged. |  | | | | | |
| **10.2.4** Invalid logical access attempts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.4** Verify invalid logical access attempts are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings verified that invalid logical access attempts are logged. |  | | | | | |
| **10.2.5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.5.a** Verify use of identification and authentication mechanisms is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings verified that use of identification and authentication mechanisms is logged. |  | | | | | |
| **10.2.5.b** Verify all elevation of privileges is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings verified that all elevation of privileges is logged. |  | | | | | |
| **10.2.5.c** Verify all changes, additions, or deletions to any account with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings verified that all changes, additions, or deletions to any account with root or administrative privileges are logged. |  | | | | | |
| **10.2.6** Initialization, stopping, or pausing of the audit logs. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.6** Verify the following are logged:   * Initialization of audit logs. * Stopping or pausing of audit logs. | *For all items in the sample at 10.2,* **describe how** configuration settings verified that initialization of audit logs is logged. |  | | | | | |
| *For all items in the sample at 10.2,* **describe how** configuration settings verified that stopping and pausing of audit logs is logged. |  | | | | | |
| **10.2.7** Creation and deletion of system-level objects. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.7** Verify creation and deletion of system level objects are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings verified that creation and deletion of system level objects are logged. |  | | | | | |
| **10.3** Record at least the following audit trail entries for all system components for each event: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following: | **Identify the responsible personnel** interviewed who confirm that for each auditable event from 10.2.1-10.2.7, the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | |
| **Identify the sample of audit logs** from 10.2.1-10.2.7 observed to verify the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | |
| **10.3.1** User identification | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.1** Verify user identification is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that user identification is included in log entries. |  | | | | | |
| **10.3.2** Type of event | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.2** Verify type of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that type of event is included in log entries. |  | | | | | |
| **10.3.3** Date and time | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.3** Verify date and time stamp is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that date and time stamp is included in log entries. |  | | | | | |
| **10.3.4** Success or failure indication | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.4** Verify success or failure indication is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verifiedsuccess or failure indication is included in log entries. |  | | | | | |
| **10.3.5** Origination of event | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.5** Verify origination of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verifiedorigination of event is included in log entries. |  | | | | | |
| **10.3.6** Identity or name of affected data, system component, or resource | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verifiedthe identity or name of affected data, system component, or resource is included in log entries. |  | | | | | |
| **10.4** Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.  ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. | **Identify** the time synchronization technologies in use. (If NTP, include version) |  | | | | | |
| **Identify** **the documented time-synchronization configuration standards** examined to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. |  | | | | | |
| **Describe how** processes were examined to verify that time synchronization technologies are: | | | | | | |
| * Implemented. |  | | | | | |
| * Kept current, per the documented process. |  | | | | | |
| **10.4.1** Critical systems have the correct and consistent time. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. * Systems receive time information only from designated central time server(s). | **Describe how** theprocess for acquiring, distributing, and storing the correct time within the organization was examined to verify the following: | | | | | | |
| * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. |  | | | | | |
| * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. |  | | | | | |
| * Systems receive time information only from designated central time server(s). |  | | | | | |
| **10.4.1.b** Observe the time-related system-parameter settings for a sample of system components to verify:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. * Systems receive time only from designated central time server(s). | **Identify the sample** of system components selected for 10.4.1.b-10.4.2.b |  | | | | | |
| *For all items in the sample,* **describe how** the time-related system-parameter settings verified: | | | | | | |
| * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. |  | | | | | |
| * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. |  | | | | | |
| * Systems receive time only from designated central time server(s). |  | | | | | |
| **10.4.2** Time data is protected. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data. | *For all items in the sample from 10.4.1,* **describe how** configuration settings verified that access to time data is restricted to only personnel with a business need to access time data. |  | | | | | |
| **10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. | *For all items in the sample from 10.4.1,* **describe how** configuration settings and time synchronization settings verified that any changes to time settings on critical systems are logged. |  | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** the examined logs verified that any changes to time settings on critical systems are logged. |  | | | | | |
| **Describe how** time synchronization processes were examined to verify changes to time settings on critical systems are: | | | | | | |
| * Logged |  | | | | | |
| * Monitored |  | | | | | |
| * Reviewed |  | | | | | |
| **10.4.3** Time settings are received from industry-accepted time sources. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers). | **Identify the sample** of time servers selected for this testing procedure. |  | | | | | |
| *For all items in the sample,* **describe how** configuration settings verified either of the following: | | | | | | |
| * That the time servers receive time updates from specific, industry-accepted external sources. OR |  | | | | | |
| * That time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines. |  | | | | | |
| **10.5** Secure audit trails so they cannot be altered. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows: | **Identify the system administrators** interviewed who confirm that audit trails are secured so that they cannot be altered as follows (from 10.5.1-10.5.5):   * Only individuals who have a job-related need can view audit trail files. * Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. * Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, including:   That current audit trail files are promptly backed up to the centralized log server or media  The frequency that audit trail files are backed up  That the centralized log server or media is difficult to alter   * Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. * Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. |  | | | | | |
| **Identify the sample** of system components selected for 10.5.1-10.5.5. |  | | | | | |
| **10.5.1** Limit viewing of audit trails to those with a job-related need. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.1** Only individuals who have a job-related need can view audit trail files. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that only individuals who have a job-related need can view audit trail files. |  | | | | | |
| **10.5.2** Protect audit trail files from unauthorized modifications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. |  | | | | | |
| **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.3** Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. |  | | | | | |
| **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.4** Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that logs for external-facing technologies are written onto a secure, centralized, internal log server or media. |  | | | | | |
| **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.5** Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs. | *For each item in the sample at 10.5,* **describe how** the following verified the use of file-integrity monitoring or change-detection software on logs: | | | | | | |
| * System settings |  | | | | | |
| * Monitored files |  | | | | | |
| * Results from monitoring activities |  | | | | | |
| **Identify** the file-integrity monitoring (FIM) or change-detection software verified to be in use. |  | | | | | |
| **10.6** Review logs and security events for all system components to identify anomalies or suspicious activity.  **Note:** Log harvesting, parsing, and alerting tools may be used to meet this Requirement. | | | | | | | |
| **10.6** Perform the following: | | | | | | | |
| **10.6.1** Review the following at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.6.1.a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | **Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | |
| **Describe** the manual or log tools used for daily review of logs. |  | | | | | |
| **10.6.1.b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | **Identify the responsible personnel** interviewed who confirm that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | | | | | | |
| * All security events. |  | | | | | |
| * Logs of all system components that store, process, or transmit CHD and/or SAD. |  | | | | | |
| * Logs of all critical system components. |  | | | | | |
| * Logs of all servers and system components that perform security functions. |  | | | | | |
| **10.6.2** Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. | **Identify** **the documented security policies and procedures** examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. |  | | | | | |
| **Describe the manual or log tools** defined for periodic review of logs of all other system components. |  | | | | | |
| **10.6.2.b** Examine the organization’s risk assessment documentation and interview personnel to verify that reviews are performed in accordance with organization’s policies and risk management strategy. | **Identify** **the organization’s risk assessment documentation** examined to verify that reviews are performed in accordance with the organization’s policies and risk management strategy. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that reviews are performed in accordance with organization’s policies and risk management strategy. |  | | | | | |
| **10.6.3** Follow up exceptions and anomalies identified during the review process. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | **Identify** **the documented security policies and procedures** examined to verify that procedures define following up on exceptions and anomalies identified during the review process. |  | | | | | |
| **10.6.3.b** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. | **Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that follow-up to exceptions and anomalies is performed. |  | | | | | |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.7.a** Examine security policies and procedures to verify that they define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. | **Identify** **the documented security policies and procedures** examined to verify that procedures define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. |  | | | | | |
| **10.7.b** Interview personnel and examine audit logs to verify that audit logs are retained for at least one year. | **Identify** **the responsible personnel** interviewed who confirm that audit logs are retained for at least one year. |  | | | | | |
| **Describe how** the audit logs verified that audit logs are retained for at least one year. |  | | | | | |
| **10.7.c** Interview personnel and observe processes to verify that at least the last three months’ logs are immediately available for analysis. | **Identify** **the responsible personnel** interviewed who confirm that at least the last three months’ logs are immediately available for analysis. |  | | | | | |
| **Describe how** processes were observed to verify that at least the last three months’ logs are immediately available for analysis. |  | | | | | |
| **10.8 *Additional requirement for service providers only*:** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:   * Firewalls * IDS/IPS * FIM * Anti-virus * Physical access controls * Logical access controls * Audit logging mechanisms * Segmentation controls (if used)   ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.8.a** Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:   * Firewalls * IDS/IPS * FIM * Anti-virus * Physical access controls * Logical access controls * Audit logging mechanisms * Segmentation controls (if used) | **Identify the documented policies and procedures** examined to verify thatprocesses are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:   * Firewalls * IDS/IPS * FIM * Anti-virus * Physical access controls * Logical access controls * Audit logging mechanisms * Segmentation controls (if used) |  | | | | | |
| **10.8.b** Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. | **Identify the responsible personnel** interviewed who confirm that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. |  | | | | | |
| **Describe how** the detection and alerting processes verified that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. |  | | | | | |
| **10.8.1 *Additional requirement for service providers only*:** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls   ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.8.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls | **Identify the documented policies and procedures** examined to verify that processes are defined and implemented to respond to a security control failure, and include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that processes are defined and implemented to respond to a security control failure, and include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls |  | | | | | |
| **10.8.1.b** Examine records to verify that security control failures are documented to include:   * Identification of cause(s) of the failure, including root cause * Duration (date and time start and end) of the security failure * Details of the remediation required to address the root cause | **Identify the sample of records** examined to verify that security control failures are documented to include:   * Identification of cause(s) of the failure, including root cause * Duration (date and time start and end) of the security failure * Details of the remediation required to address the root cause |  | | | | | |
| *For each sampled record,* **describe how** the documented security control failures include:   * Identification of cause(s) of the failure, including root cause * Duration (date and time start and end) of the security failure * Details of the remediation required to address the root cause |  | | | | | |
| **10.9** Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.9** Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for monitoring all access to network resources and cardholder data are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 11: Regularly test security systems and processes

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.  **Note:** Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.  Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.a** Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis. | **Identify** **the documented policies and procedures** examined to verify processes are defined for detection and identification of authorized and unauthorized wireless access points on a quarterly basis. |  | | | | | |
| **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:   * WLAN cards inserted into system components. * Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). * Wireless devices attached to a network port or network device. | **Provide the name of the assessor** who attests that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:   * WLAN cards inserted into system components. * Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). * Wireless devices attached to a network port or network device. |  | | | | | |
| **11.1.c If wireless scanning is utilized,** examine output from recent wireless scans to verify that:   * Authorized and unauthorized wireless access points are identified, and * The scan is performed at least quarterly for all system components and facilities. | **Indicate whether** wireless scanning is utilized. **(yes/no)**  *If ‘no,’ mark the remainder of 11.1.c as ‘not applicable.’* |  | | | | | |
| *If ‘yes,’* **Identify/describe** the output from recent wireless scans examined to verify that:   * Authorized wireless access points are identified. * Unauthorized wireless access points are identified. * The scan is performed at least quarterly. * The scan covers all system components. * The scan covers all facilities. |  | | | | | |
| **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel. | **Indicate** **whether** automated monitoring is utilized. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 11.1.d as “Not Applicable.”*  *If “yes,” complete the following:* | | | | | | |
| **Identify and describe** any automated monitoring technologies in use. |  | | | | | |
| *For each monitoring technology in use,* **describe how** the technology generates alerts to personnel. |  | | | | | |
| **11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.1** Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. | **Identify** **the documented inventory records** of authorized wireless access points examined to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. |  | | | | | |
| **11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.2.a** Examine the organization’s incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected. | **Identify the Incident Response Plan document** examined that defines and requires response in the event that an unauthorized wireless access point is detected. |  | | | | | |
| **11.1.2.b** Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found. | **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that action is taken when unauthorized wireless access points are found. |  | | | | | |
| *And/or:* | | | | | | |
| **Identify the recent wireless scans** inspected for this testing procedure. |  | | | | | |
| **Describe how** the recent wireless scans and related responses verified that action is taken when unauthorized wireless access points are found. |  | | | | | |
| **11.2** Run internal and external network vulnerability scans at least quarterly andafter any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).  **Note:** Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.  For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2** Examine scan reports and supporting documentation toverify that internal and external vulnerability scans are performed as follows: | | | | | | | |
| **11.2.1** Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high-risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. | **Identify** **the internal vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly internal scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.1.b** Review the scan reports and verify that all “high-risk” vulnerabilities are addressed and the scan process includes rescans to verify that the “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | **Identify the documented process for quarterly internal scanning** to verify the process defines performing rescans as part of the quarterly internal scan process. |  | | | | | |
| *For each of the four internal quarterly scans indicated at 11.2.1.a*, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes,”* **describe how** rescans were verified to be performed until all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. |  | | | | | |
| **11.2.1.c** Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Identify the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| **Indicate** **whether** a qualified internal resource performs the scan. **(yes/no)**  *If “no,” mark the remainder of 11.2.1.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify: | | | | | | |
| * The scan was performed by a qualified internal resource |  | | | | | |
| * Organizational independence of the tester exists. |  | | | | | |
| **11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.  **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).  Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period. | **Identify** **the external network vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly external vulnerability scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.2.b** Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures). | **Provide the name of the assessor** who attests that the results of each quarterly scan were reviewed and verified that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| *For each of the four external quarterly scans indicated at 11.2.2.a*, **indicate whether** a rescan was necessary. **(yes/no)** |  | | | | | |
| *If “yes,”* **describe how** the results of the rescan verified that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| **11.2.2.c** Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV). | **Provide the name of the assessor** who attests that the external scan reports were reviewed and verified to have been completed by a PCI SSC-Approved Scanning Vendor (ASV). |  | | | | | |
| **11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.3.a** Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned. | **Identify the change control documentation and scan reports** reviewed for this testing procedure. |  | | | | | |
| **Describe how** the change control documentation and scan reports verified that all system components subject to significant change were scanned after the change. |  | | | | | |
| **11.2.3.b** Review scan reports and verify that the scan process includes rescans until:   * For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. * For internal scans, all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | For all scans reviewed in 11.2.3.a, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes”* – for external scans, **describe how** rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist. |  | | | | | |
| *If “yes”* – for internal scans, **describe how** rescans were performed until either passing results were obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved. |  | | | | | |
| **11.2.3.c** Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Indicate whether** an **i**nternal resource performed the scans. **(yes/no)**  *If “no,” mark the remainder of 11.2.3.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the scans demonstrated they are qualified to perform the scans. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3** Implement a methodology for penetration testing that includes at least the following:   * Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside of the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3** Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented and includes at least the following:   * Is based on industry-accepted penetration testing approaches. * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results. | **Identify the documented penetration-testing methodology** examined to verify a methodology is implemented that includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
|  | **Identify the responsible personnel** interviewed who confirm the penetration–testing methodology implemented includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
| **11.3.1** Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.1.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented external penetration test results** reviewed to verify that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work verified that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Identify whether** any significant external infrastructure or application upgrade or modification occurred during the past 12 months. |  | | | | | |
| **Identify** **the documented penetration test results reviewed** to verify that external penetration tests are performed after significant external infrastructure or application upgrade. |  | | | | | |
| **11.3.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Indicate whether** an **i**nternal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.1.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.2** Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented internal penetration test results** reviewed to verify that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work verified that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Indicate whether** any significant internal infrastructure or application upgrade or modification occurred during the past 12 months. **(yes/no)** |  | | | | | |
| **Identify** **the documented internal penetration test results** reviewed to verify that internal penetration tests are performed after significant internal infrastructure or application upgrade. |  | | | | | |
| **11.3.2.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Indicate whether** an **i**nternal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.2.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.3** Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.3** Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. | **Identify the documented penetration testing results** examined to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. |  | | | | | |
| **11.3.4** If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.4.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Indicate** **whether** segmentation is used to isolate the CDE from other networks. **(yes/no)**  *If “no,” mark the remainder of 11.3.4.a and 11.3.4.b as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **identify the defined penetration-testing methodology** examined to verify procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **Describe how** the segmentation controls verified that segmentation methods: | | | | | | |
| * Are operational and effective. |  | | | | | |
| * Isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.3.4.b** Examine the results from the most recent penetration test to verify that:   * Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Identify the documented results from the most recent penetration test** examined to verify that:   * Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.3.4.c** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.4.1 *Additional requirement for service providers only:*** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.  ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.4.1.a** Examine the results from the most recent penetration test to verify that:   * Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Identify the documented results from the most recent penetration test** examined to verify that:   * Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.3.4.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.4** Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.  Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. | **Identify the network diagrams** examined to verify that techniques are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. |  | | | | | |
| **Describe how** system configurations verified that techniques are in place to monitor all traffic: | | | | | | |
| * At the perimeter of the cardholder data environment. |  | | | | | |
| * At critical points in the cardholder data environment. |  | | | | | |
| **11.4.b** Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. | **Describe how** system configurations for intrusion-detection and/or intrusion-prevention techniques verified that they are configured to alert personnel of suspected compromises. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the generated alerts are received as intended. |  | | | | | |
| **11.4.c** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | **Identify** **the vendor document(s)** examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques. |  | | | | | |
| **Describe how** IDS/IPS configurations and vendor documentation verified that intrusion-detection, and/or intrusion-prevention techniques are: | | | | | | |
| * Configured per vendor instructions to ensure optimal protection. |  | | | | | |
| * Maintained per vendor instructions to ensure optimal protection. |  | | | | | |
| * Updated per vendor instructions to ensure optimal protection. |  | | | | | |
| **11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.  **Note:** For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.a** Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities.  *Examples of files that should be monitored:*   * *System executables* * *Application executables* * *Configuration and parameter files* * *Centrally stored, historical or archived, log and audit files* * *Additional critical files determined by entity (i.e., through risk assessment or other means)* | **Describe** the change-detection mechanism deployed. |  | | | | | |
| **Identify the results** from monitored files reviewed to verify the use of a change-detection mechanism. |  | | | | | |
| **Describe how** the following verified the use of a change-detection mechanism: | | | | | | |
| * System settings |  | | | | | |
| * Monitored files |  | | | | | |
| **11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly. | **Describe how** system settings verified that the change-detection mechanism is configured to: | | | | | | |
| * Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files. |  | | | | | |
| * Perform critical file comparisons at least weekly. |  | | | | | |
| **11.5.1** Implement a process to respond to any alerts generated by the change-detection solution. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.1** Interview personnel to verify that all alerts are investigated and resolved. | **Identify the responsible personnel** interviewed who confirm that all alerts are investigated and resolved |  | | | | | |
| **11.6** Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.6** Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for security monitoring and testing are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for security monitoring and testing are:   * In use * Known to all affected parties |  | | | | | |

### Maintain an Information Security Policy

#### Requirement 12: Maintain a policy that addresses information security for all personnel

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **12.1** Establish, publish, maintain, and disseminate a security policy. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  | | | | | |
| **Describe how** the information security policy was verified to be published and disseminated to: | | | | | | |
| * All relevant personnel. |  | | | | | |
| * All relevant vendors and business partners. |  | | | | | |
| **12.1.1** Review the security policy at least annually and update the policy when business objectives or the risk environment change. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1.1** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | **Describe how** the information security policy was verified to be: | | | | | | |
| * Reviewed at least annually. |  | | | | | |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  | | | | | |
| **12.2** Implement a risk assessment process, that:   * Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), * Identifies critical assets, threats, and vulnerabilities, and * Results in a formal, documented analysis of risk.   *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.2.a** Verify that an annual risk-assessment process is documented that:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. | **Provide the name of the assessor** who attests that the documented annual risk-assessment process:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. |  | | | | | |
| **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | **Identify the risk assessment result documentation** reviewed to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. |  | | | | | |
| **12.3** Develop usage policies for critical technologies and define proper use of these technologies.  **Note:** Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.  Ensure these usage policies require the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed: | **Identify** critical technologies in use. |  | | | | | |
| **Identify the usage policies for all identified critical technologies** reviewed to verify the following policies (12.3.1-12.3.10) are defined:   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **Identify the responsible** **personnel** interviewed who confirm usage policies for all identified critical technologies are implemented and followed (for 12.3.1–12.3.10):   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.1** Explicit approval by authorized parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.1** Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to include processes for explicit approval from authorized parties to use the technologies. |  | | | | | |
| **12.3.2** Authentication for use of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.2** Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token). | **Provide the name of the assessor** who attests that the usage policies were verified to include processes for all technology use to be authenticated with user ID and password or other authentication item. |  | | | | | |
| **12.3.3** A list of all such devices and personnel with access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.3** Verify that the usage policies define:   * A list of all critical devices, and * A list of personnel authorized to use the devices. | **Provide the name of the assessor** who attests that the usage policies were verified to define:   * A list of all critical devices, and * A list of personnel authorized to use the devices. |  | | | | | |
| **12.3.4** A method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.4** Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | **Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine:   * Owner * Contact Information * Purpose |  | | | | | |
| **12.3.5** Acceptable uses of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.5** Verify that the usage policies define acceptable uses for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  | | | | | |
| **12.3.6** Acceptable network locations for the technologies. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.6** Verify that the usage policies define acceptable network locations for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable network locations for the technology. |  | | | | | |
| **12.3.7** List of company-approved products. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.7** Verify that the usage policies include a list of company-approved products. | **Provide the name of the assessor** who attests that the usage policies were verified to include a list of company-approved products. |  | | | | | |
| **12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.8.a** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | **Provide the name of the assessor** who attests that the usage policies were verified to require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. |  | | | | | |
| **12.3.8.b** Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity. | **Identify** any remote access technologies in use |  | | | | | |
| . **Describe how** configurations for remote access technologies verified that remote access sessions will be automatically disconnected after a specific period of inactivity. |  | | | | | |
| **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | **Provide the name of the assessor** who attests that the usage policies were verified to require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. |  | | | | | |
| **12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to prohibit copying, moving or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements. | **Provide the name of the assessor** who attests that the usage policies were verified to require, for personnel with proper authorization, the protection of cardholder data in accordance with PCI DSS Requirements. |  | | | | | |
| **12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.4.a** Verify that information security policy and procedures clearly define information security responsibilities for all personnel. | **Identify** **the information security policy and procedures** reviewed to verify that they clearly define information security responsibilities for all personnel. |  | | | | | |
| **12.4.b** Interview a sample of responsible personnel to verify they understand the security policies. | **Identify the responsible personnel** interviewed for this testing procedure who confirm they understand the security policy. |  | | | | | |
| **12.4.1 *Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:   * Overall accountability for maintaining PCI DSS compliance * Defining a charter for a PCI DSS compliance program and communication to executive management   ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.4.1.a** Examine documentation to verify executive management has assigned overall accountability for maintaining the entity’s PCI DSS compliance | **Identify the documentation** examined to verify thatexecutive management has assigned overall accountability for maintaining the entity’s PCI DSS compliance. |  | | | | | |
| **12.4.1.b** Examine the company’s PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management. | **Identify the company’s PCI DSS charter** examined to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management. |  | | | | | |
| **12.5** Assign to an individual or team the following information security management responsibilities: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5** Examine information security policies and procedures to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: | **Identify** **the information security policies and procedures** reviewed to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: |  | | | | | |
| **12.5.1** Establish, document, and distribute security policies and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.1** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security policies and procedures. * Documenting security policies and procedures. * Distributing security policies and procedures. |  | | | | | |
| **12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring and analyzing security alerts. * Distributing information to appropriate information security and business unit management personnel. |  | | | | | |
| **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.3** Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security incident response and escalation procedures. * Documenting security incident response and escalation procedures. * Distributing security incident response and escalation procedures. |  | | | | | |
| **12.5.4** Administer user accounts, including additions, deletions, and modifications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.4** Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for administering user account and authentication management. |  | | | | | |
| **12.5.5** Monitor and control all access to data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring all access to data * Controlling all access to data |  | | | | | |
| **12.6** Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.a** Review the security awareness program to verify it provides awareness to all personnel about the cardholder data security policy and procedures. | **Provide the name of the assessor** who attests that the security awareness program was verified to provide awareness to all personnel about the cardholder data security policy and procedures. |  | | | | | |
| **12.6.b** Examine security awareness program procedures and documentation and perform the following: | **Identify the documented security awareness program procedures and additional documentation** examined to verify that:   * The security awareness program provides multiple methods of communicating awareness and educating personnel. * Personnel attend security awareness training:   Upon hire, and  At least annually   * Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. |  | | | | | |
| **12.6.1** Educate personnel upon hire and at least annually.  ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel. |  | | | | | |
| **12.6.1.b** Verify that personnel attend security awareness training upon hire and at least annually. | **Describe how** it was observed that all personnel attend security awareness training: | | | | | | |
| * Upon hire |  | | | | | |
| * At least annually |  | | | | | |
| **12.6.1.c** Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security. | **Identify the sample** of personnel interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify they have completed awareness training and are aware of the importance of cardholder data security. |  | | | | | |
| **12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. | **Describe how** it was observed that, per the security awareness program, all personnel: | | | | | | |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  | | | | | |
| * Provide an acknowledgement at least annually. |  | | | | | |
| **12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)  **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. | **Identify the Human Resources personnel** interviewed who confirm background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  | | | | | |
| **Describe how** it was observed that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  | | | | | |
| **12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8**Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows: | **Identify the documented policies and procedures** reviewed to verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, per 12.8.1–12.8.5: |  | | | | | |
| **12.8.1** Maintain a list of service providers including a description of the service provided. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.1** Verify that a list of service providers is maintained and includes a list of the services provided. | **Describe how** the documented list of service providers was observed to be maintained (kept up-to-date) and includes a list of the services provided. |  | | | | | |
| **12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE.  ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.2** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | **Describe how** written agreements for each service provider were observed to include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer. |  | | | | | |
| **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Identify the policies and procedures** reviewed to verify that processes included proper due diligence prior to engaging any service provider. |  | | | | | |
| **Describe how** it was observed that the above policies and procedures are implemented. |  | | | | | |
| **12.8.4** Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.4** Verify that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. | **Describe how** it was observed that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. |  | | | | | |
| **12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.5** Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | **Describe how** it was observed that the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  | | | | | |
| **12.9 *Additional requirement for service providers only*:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.  **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.9 *Additional testing procedure for service provider assessments only****:*Review service provider’s policies and procedures and observe templates used for written agreement to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | **Indicate whether** the assessed entity is a service provider. **(yes/no)**  *If “no,” mark the remainder of 12.9 as “Not Applicable.”*  *If “yes”:* |  | | | | | |
| **Identify the service provider’s policies and procedures** reviewed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **Describe how** the templates used for written agreement verified that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following: | **Identify** **the documented incident response plan and related procedures** examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows from 12.10.1–12.10.6:   * Create the incident response plan to be implemented in the event of system breach. * Test the plan at least annually. * Designate specific personnel to be available on a 24/7 basis to respond to alerts:   24/7 incident monitoring  24/7 incident response   * Provide appropriate training to staff with security breach response responsibilities. * Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. * Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  | | | | | |
| **12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:   * Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage and responses of all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.1.a** Verify that the incident response plan includes:   * Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures * Data back-up processes * Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). * Coverage and responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  | | | | | |
| **12.10.1.b** Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed. | **Identify the responsible** **personnel** interviewed who confirm that the documented incident response plan and procedures are followed. |  | | | | | |
| **Identify the sample** of previously reported incidents or alerts selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** the documented incident response plan and procedures were observed to be followed. |  | | | | | |
| **12.10.2** Review and test the plan at least annually, including all elements listed in Requirement 12.10.1. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.2** Interview personnel and review documentation from testing to verify that the plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1. | **Identify the responsible personnel** interviewed who confirm that the incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1. |  | | | | | |
| **Identify documentation** reviewed from testing to verify thatthe incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1. |  | | | | | |
| **12.10.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes. | **Identify** **the document** requiring 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
|  | | | | | | |
| **Describe how** it was observed that designated personnel are available for 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **12.10.4** Provide appropriate training to staff with security breach response responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.4** Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained. | **Identify the responsible personnel** interviewed who confirm that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Identify the documented policy** reviewed to verify that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Describe how** it was observed that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **12.10.5** Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan. | **Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **Describe how** processes were reviewed to verify that ***responding to*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **12.10.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.6** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | | | | | | |
| * According to lessons learned. |  | | | | | |
| * To incorporate industry developments. |  | | | | | |
| **12.11 *Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:   * Daily log reviews * Firewall rule-set reviews * Applying configuration standards to new systems * Responding to security alerts * Change management processes   ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.11.a** Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover:   * Daily log reviews * Firewall rule-set reviews * Applying configuration standards to new systems * Responding to security alerts * Change management processes | **Identify the policies and procedures** examined to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover:   * Daily log reviews * Firewall rule-set reviews * Applying configuration standards to new systems * Responding to security alerts * Change management processes |  | | | | | |
| **12.11.b** Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly | **Identify the document(s) related to reviews** examined to verify that reviews are performed at least quarterly. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that reviews are performed at least quarterly |  | | | | | |
| **12.11.1** ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include:   * Documenting results of the reviews * Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program   ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.11.1.a** Examine documentation from the quarterly reviews to verify they include:   * Documenting results of the reviews. * Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program. | **Identify the document(s) related to quarterly reviews** to verify they include:   * Documenting results of the reviews. * Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program. |  | | | | | |

## PCI DSS v3.2.1

### Build and Maintain a Secure Network and Systems

#### Requirement 1: Install and maintain a firewall configuration to protect cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings** (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **1.1** Establish and implement firewall and router configuration standards that include the following: | | | | | | | |
| **1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows: | | | | | | | |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all:   * Network connections, and * Changes to firewall and router configurations. | **Identify the document(s)** reviewed to verify procedures define the formal processes for: | | | | | | |
| * Testing and approval of all network connections. |  | | | | | |
| * Testing and approval of all changes to firewall and router configurations. |  | | | | | |
| **1.1.1.b** For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested. | **Identify the sample of records** for network connections that were selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that network connections were approved and tested. |  | | | | | |
| **Describe how** the sampled records verified that network connections were: | | | | | | |
| * Approved |  | | | | | |
| * Tested |  | | | | | |
| **1.1.1.c** Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested. | **Identify** **the sample of records** for firewall and router configuration changes that were selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that changes made to firewall and router configurations were approved and tested. |  | | | | | |
| **Describe how** the sampled records verified that the firewall and router configuration changes were: | | | | | | |
| * Approved |  | | | | | |
| * Tested |  | | | | | |
| **1.1.2** Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to the cardholder data environment, including any wireless networks. | **Identify the current network diagram**(s) examined. |  | | | | | |
| **Describe how** network configurations verified that the diagram: | | | | | | |
| * Is current. |  | | | | | |
| * Includes all connections to cardholder data. |  | | | | | |
| * Includes any wireless network connections. |  | | | | | |
| **1.1.2.b** Interview responsible personnel to verify that the diagram is kept current. | **Identify** **the responsible personnel** interviewed who confirm that the diagram is kept current. |  | | | | | |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.3.a** Examine data flow diagram and interview personnel to verify the diagram:   * Shows all cardholder data flows across systems and networks. * Is kept current and updated as needed upon changes to the environment. | **Identify** **the data-flow diagram**(s) examined. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that the diagram:   * Shows all cardholder data flows across systems and networks. * Is kept current and updated as needed upon changes to the environment. |  | | | | | |
| **1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.4.a** Examine thefirewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. | **Identify** **the firewall configuration standards document** examined to verify requirements for a firewall:   * At each Internet connection. * Between any DMZ and the internal network zone. |  | | | | | |
| **1.1.4.b** Verify that the current network diagram is consistent with the firewall configuration standards. | **Provide the name of the assessor** who attests that the current network diagram is consistent with the firewall configuration standards. |  | | | | | |
| **1.1.4.c** Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams. | **Describe how** network configurations verified that, per the documented configuration standards and network diagrams, a firewall is in place: | | | | | | |
| * At each Internet connection. |  | | | | | |
| * Between any DMZ and the internal network zone. |  | | | | | |
| **1.1.5** Description of groups, roles, and responsibilities for management of network components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify they include a description of groups, roles and responsibilities for management of network components. |  | | | | | |
| **1.1.5.b** Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented. | **Identify the responsible personnel** interviewed who confirm that roles and responsibilities are assigned as documented. |  | | | | | |
| **1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification and approval for each. |  | | | | | |
| **1.1.6.b** Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. | **Indicate whether** any insecure services, protocols or ports are allowed. **(yes/no)** |  | | | | | |
| If “yes,” complete the instructions below for EACH insecure service, protocol, and port allowed: (add rows as needed) | | | | | | |
| **Identify the firewall and router configuration standards** **document(s)** reviewed to verify that security features are documented for each insecure service/protocol/port. |  | | | | | |
| **1.1.6.c** Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port. | If “yes” at 1.1.6.b, complete the following for each insecure service, protocol, and/or port present (add rows as needed): | | | | | | |
| **Describe how** firewall and router configurations verified that the documented security features are implemented for each insecure service, protocol and/or port. |  | | | | | |
| **1.1.7** Requirement to review firewall and router rule sets at least every six months. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.7.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify they require a review of firewall rule sets at least every six months. |  | | | | | |
| **1.1.7.b** Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. | **Identify the document(s) relating to rule set reviews** that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.  **Note:** An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. | | | | | | | |
| **1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment: | | | | | | | |
| **1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.1.a** Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment. | **Identify the firewall and router configuration standards document(s)** reviewed to verify they identify inbound and outbound traffic necessary for the cardholder data environment. |  | | | | | |
| **1.2.1.b** Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment. | **Describe how** firewall and router configurations verified that the following traffic is limited to that which is necessary for the cardholder data environment: | | | | | | |
| * Inbound traffic |  | | | | | |
| * Outbound traffic |  | | | | | |
| **1.2.1.c** Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement. | **Describe how** firewall and router configurations verified that the following is specifically denied: | | | | | | |
| * All other inbound traffic |  | | | | | |
| * All other outbound traffic |  | | | | | |
| **1.2.2** Secure and synchronize router configuration files. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access. | **Describe how** router configuration files are secured from unauthorized access. |  | | | | | |
| **1.2.2.b** Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted). | **Describe how** router configurations are synchronized. |  | | | | | |
| **1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment. | **Describe how** firewall and router configurations verified that perimeter firewalls are in place between all wireless networks and the cardholder data environment. |  | | | | | |
| **1.2.3.b** Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | **Indicate whether** traffic between the wireless environment and the cardholder data environment is necessary for business purposes. **(yes/no)** |  | | | | | |
| *If “no”:* | | | | | | |
| **Describe how** firewall and/or router configurations verified that firewalls deny all traffic from any wireless environment into the cardholder environment. |  | | | | | |
| *If “yes”:* | | | | | | |
| **Describe how** firewall and/or router configurations verified that firewalls permit only authorized traffic from any wireless environment into the cardholder environment. |  | | | | | |
| **1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment. | | | | | | | |
| **1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment: | | | | | | | |
| **1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | **Describe how** firewall and router configurations verified that the DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. |  | | | | | |
| **1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ. | **Describe how** firewall and router configurations verified that configurations limit inbound Internet traffic to IP addresses within the DMZ. |  | | | | | |
| **1.3.3** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.  (For example, block traffic originating from the Internet with an internal source address) | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.3** Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ. | **Describe how** firewall and router configurations verified that anti-spoofing measures are implemented. |  | | | | | |
| **1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.4** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. | **Describe how** firewall and router configurations verified that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. |  | | | | | |
| **1.3.5** Permit only “established” connections into the network. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.5** Examine firewall and router configurations to verify that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session. | **Describe how** firewall and router configurations verified that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session |  | | | | | |
| **1.3.6** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.6** Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. | **Indicate whether** any system components store cardholder data. **(yes/no)** |  | | | | | |
| *If “yes”:* | | | | | | |
| **Describe how** firewall and router configurations verified that the system components that store cardholder data are located on an internal network zone, and are segregated from the DMZ and other untrusted networks. |  | | | | | |
| **1.3.7** Do not disclose private IP addresses and routing information to unauthorized parties.  Note: Methods to obscure IP addressing may include, but are not limited to:   * Network Address Translation (NAT), * Placing servers containing cardholder data behind proxy servers/firewalls, * Removal or filtering of route advertisements for private networks that employ registered addressing, * Internal use of RFC1918 address space instead of registered addresses. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.7.a** Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. | **Describe how** firewall and router configurations verified that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |  | | | | | |
| **1.3.7.b** Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized. | **Identify the document** reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted. |  | | | | | |
| For each permitted disclosure, **identify the responsible personnel** interviewed who confirm that the disclosure is authorized. |  | | | | | |
| **1.4** Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:   * Specific configuration settings are defined. * Personal firewall (or equivalent functionality) is actively running. * Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.4.a** Examinepolicies andconfiguration standards to verify:   * Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. * Specific configuration settings are defined for personal firewall or equivalent functionality. * Personal firewall or equivalent functionality is configured to actively run. * Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices. | **Indicate whether** portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network are used to access the organization’s CDE. **(yes/no)** |  | | | | | |
| *If “no,”* **identify** **the document** reviewed that explicitly prohibits portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network from being used to access the organization’s CDE.  *Mark 1.4.b as “not applicable”* |  | | | | | |
| *If “yes,”* **identify** **the documented policies and configuration standards** that define the following:   * Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. * Specific configuration settings are defined for personal firewall or equivalent functionality. * Personal firewall or equivalent functionality is configured to actively run. * Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices. |  | | | | | |
| **1.4.b** Inspect a sample of portable computing devices (including company and/or employee-owned) to verify that:   * Personal firewall (or equivalent functionality) is installed and configured per the organization’s specific configuration settings. * Personal firewall (or equivalent functionality) is actively running. * Personal firewall or equivalent functionality is not alterable by users of the portable computing devices. | **Identify the sample** of mobile and/or employee-owned devices selected for this testing procedure. |  | | | | | |
| **Describe how** the sample of portable computing devices (including company and/or employee-owned) verified that personal firewall software is: | | | | | | |
| * Installed and configured per the organization’s specific configuration settings. |  | | | | | |
| * Actively running. |  | | | | | |
| * Not alterable by users of mobile and/or employee-owned devices. |  | | | | | |
| **1.5** Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed** to verify that security policies and operational procedures for managing firewalls are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing firewalls are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.  This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.a** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| **Identify** **the vendor manuals and sources on the Internet** used to find vendor-supplied accounts/passwords. |  | | | | | |
| *For each item in the sample*, **describe how** attempts to log on to the sample of devices and applications using default vendor-supplied accounts and passwords verified that all default passwords have been changed. |  | | | | | |
| **2.1.b** For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled. | For each item in the sample of system components indicated at 2.1.a, **describe how** all unnecessary default accounts were verified to be **either**: | | | | | | |
| * Removed |  | | | | | |
| * Disabled |  | | | | | |
| **2.1.c** Interview personnel and examine supporting documentation to verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. | **Identify the responsible personnel** interviewed who verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. |  | | | | | |
| **Identify supporting documentation** examined to verify that:   * All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. * Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network. |  | | | | | |
| **2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.1.a** Interview responsible personnel and examine supporting documentation to verify that:   * Encryption keys were changed from default at installation * Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. | **Indicate whether** there are wireless environments connected to the cardholder data environment or transmitting cardholder data. **(yes/no)**  *If “no,” mark 2.1.1 as “Not Applicable” and proceed to 2.2.* |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify the responsible personnel** interviewed who verify that encryption keys are changed:   * From default at installation * Anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **Identify supporting documentation** examined to verify that:   * Encryption keys were changed from default at installation * Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **2.1.1.b** Interview personnel and examine policies and procedures to verify:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. | **Identify the responsible personnel** interviewed who verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/passphrases on access points are required to be changed upon installation. |  | | | | | |
| **Identify policies and procedures** examined to verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. |  | | | | | |
| **2.1.1.c** Examine vendor documentation and login to wireless devices, with system administrator help, to verify:   * Default SNMP community strings are not used. * Default passwords/passphrases on access points are not used. | **Identify** **vendor documentation** examined to verify that:   * Default SNMP community strings are not used. * Default passwords/passphrases on access points are not used. |  | | | | | |
| **Describe how** attempts to login to wireless devices verified that: | | | | | | |
| * Default SNMP community strings are not used. |  | | | | | |
| * Default passwords/passphrases on access points are not used. |  | | | | | |
| **2.1.1.d** Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for:   * Authentication over wireless networks * Transmission over wireless networks | **Identify** **vendor documentation** examined to verify firmware on wireless devices is updated to support strong encryption for:   * Authentication over wireless networks * Transmission over wireless networks |  | | | | | |
| **Describe how** wireless configuration settings verified that firmware on wireless devices is updated to support strong encryption for: | | | | | | |
| * Authentication over wireless networks. |  | | | | | |
| * Transmission over wireless networks. |  | | | | | |
| **2.1.1.e** Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable. | **Identify** **vendor documentation** examined to verify other security-related wireless vendor defaults were changed, if applicable. |  | | | | | |
| **Describe how** wireless configuration settings verified that other security-related wireless vendor defaults were changed, if applicable. |  | | | | | |
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.  Sources of industry-accepted system hardening standards may include, but are not limited to:   * Center for Internet Security (CIS) * International Organization for Standardization (ISO) * SysAdmin Audit Network Security (SANS) Institute * National Institute of Standards Technology (NIST) | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.a** Examine the organization’s system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. | **Identify** **the documented system configuration standards** for all types of system components examined to verify the system configuration standards are consistent with industry-accepted hardening standards. |  | | | | | |
| **Provide the name of the assessor** who attests that the system configuration standards are consistent with industry-accepted hardening standards. |  | | | | | |
| **2.2.b** Examine policies and interview personnel toverify thatsystem configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. | **Identify** **the policy documentation** examined toverify thatsystem configuration standards are updated as new vulnerability issues are identified. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm thatsystem configuration standards are updated as new vulnerability issues are identified. |  | | | | | |
| **2.2.c** Examine policies and interview personnel toverify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. | **Identify** **the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. |  | | | | | |
| **2.2.d** Verify that system configuration standards include the following procedures for all types of system components:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers | **Identify the system configuration standards** for all types of system components that include the following procedures:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers |  | | | | | |
| **2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)  **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** system configurations verified that only one primary function per server is implemented. |  | | | | | |
| **2.2.1.b** If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device. | **Indicate** **whether** virtualization technologies are used. **(yes/no)** |  | | | | | |
| *If “no,”* **describe how** systems were observed to verify that no virtualization technologies are used. |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify the sample** of virtual system components or devices selected for this testing procedure. |  | | | | | |
| *For each virtual system component and device in the sample*, **describe how** system configurations verified that only one primary function is implemented per virtual system component or device. |  | | | | | |
| **2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** the enabled system services, daemons, and protocols verified that only necessary services or protocols are enabled. |  | | | | | |
| **2.2.2.b** Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards. | *For each item in the sample of system components from 2.2.2.a,* **indicate whether** any insecure services, daemons, or protocols are enabled. **(yes/no)**  *If “no,” mark the remainder of 2.2.2.b and 2.2.3 as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **identify the responsible personnel** interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol |  | | | | | |
| **2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.3** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. | *If “yes” at 2.2.2.b, perform the following:* | | | | | | |
| **Describe how** configuration settings verified that security features for all insecure services, daemons, or protocols are: | | | | | | |
| * Documented |  | | | | | |
| * Implemented |  | | | | | |
| **2.2.4** Configure system security parameters to prevent misuse. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.4.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components. | **Identify the system administrators and/or security managers** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed to verify that they have knowledge of common security parameter settings for system components. |  | | | | | |
| **2.2.4.b** Examine the system configuration standards to verify that common security parameter settings are included. | **Identify** **the system configuration standards** examined to verify that common security parameter settings are included. |  | | | | | |
| **2.2.4.c** Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** the common security parameters verified that they are set appropriately and in accordance with the configuration standards. |  | | | | | |
| **2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** configurations verified that all unnecessary functionality is removed. |  | | | | | |
| **2.2.5.b** Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration. | **Describe how** the security parameters and relevant documentation verified that enabled functions are: | | | | | | |
| * Documented |  | | | | | |
| * Support secure configuration |  | | | | | |
| **2.2.5.c** Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components. | **Identify** **documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the security parameters verified that only documented functionality is present on the sampled system components from 2.2.5.a. |  | | | | | |
| **2.3** Encrypt all non-console administrative access using strong cryptography. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: | **Identify the sample** of system components selected for 2.3.a-2.3.d. |  | | | | | |
| **2.3.a** Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator’s password is requested. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on to each system verified that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Describe how** system configurations for each system verified that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Identify** **the strong encryption method** used for non-console administrative access. |  | | | | | |
| **2.3.b** Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** services and parameter files on systems verified that Telnet and other insecure remote-login commands are not available for non-console access. |  | | | | | |
| **2.3.c** Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on to each system verified that administrator access to any web-based management interfaces was encrypted with strong cryptography. |  | | | | | |
| **Identify** **the strong encryption method** used for any web-based management interfaces. |  | | | | | |
| **2.3.d** Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. | **Identify** **the vendor documentation** examined to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **2.4** Maintain an inventory of system components that are in scope for PCI DSS. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. | **Describe how** the system inventory verified that a list of hardware and software components is: | | | | | | |
| * Maintained |  | | | | | |
| * Includes a description of function/use for each |  | | | | | |
| **2.4.b** Interview personnel to verify the documented inventory is kept current. | **Identify** **the responsible personnel** interviewed who confirm that the documented inventory is kept current. |  | | | | | |
| **2.5** Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for managing vendor defaults and other security parameters are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing vendor defaults and other security parameters are:   * In use * Known to all affected parties |  | | | | | |
| **2.6** Shared hosting providers must protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.6** Perform testing procedures **A1.1** through **A1.4** detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities’ (merchants and service providers) hosted environment and data. | **Indicate** **whether** the assessed entity is a shared hosting provider. **(yes/no)** |  | | | | | |
| *If “yes,”* **provide the name of the assessor** who attests that Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers has been completed. |  | | | | | |

### Protect Stored Cardholder Data

#### Requirement 3: Protect stored cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **3.1** Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific retention requirements for cardholder data * Processes for secure deletion of data when no longer needed. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.1.a** Examine the data-retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. | **Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. * Specific requirements for retention of cardholder data. * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. |  | | | | | |
| **3.1.b** Interview personnel to verify that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. | **Identify the responsible personnel** interviewed who confirm that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. |  | | | | | |
| **3.1.c** For a sample of system components that store cardholder data:   * Examine files and system records to verify that the data stored does not exceed the requirements defined in the data-retention policy. * Observe the deletion mechanism to verify data is deleted securely. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** files and system records verified that the data stored does not exceed the requirements defined in the data-retention policy. |  | | | | | |
| **Describe how** the deletion mechanism was observed to verify data is deleted securely. |  | | | | | |
| **3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.  It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:   * There is a business justification, and * The data is stored securely.   Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. | **Indicate whether** the assessed entity is an issuer or supports issuing service. **(yes/no)** |  | | | | | |
| *If “yes,” complete the responses for 3.2.a and 3.2.b and mark 3.2.c and 3.2.d as “Not Applicable.”*  *If “no,” mark the remainder of 3.2.a and 3.2.b as “Not Applicable” and proceed to 3.2.c and 3.2.d.* | | | | | | |
| **Identify** **the documentation** reviewed to verify there is a documented business justification for the storage of sensitive authentication data. |  | | | | | |
| **Identify** **the interviewed personnel** who confirm there is a documented business justification for the storage of sensitive authentication data. |  | | | | | |
| For the interview, **summarize the relevant details** of the business justification described. |  | | | | | |
| **3.2.b** For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. | *If “yes” at 3.2.a,* | | | | | | |
| **Identify** **data stores** examined. |  | | | | | |
| **Describe how** the data stores and system configurations were examined to verify that the sensitive authentication data is secured. |  | | | | | |
| **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization. | **Indicate whether** sensitive authentication data is received. **(yes/no)** |  | | | | | |
| *If “yes,” complete 3.2.c and 3.2.d.*  *If “no,” mark the remainder of 3.2.c and 3.2.d as “Not Applicable” and proceed to 3.2.1.* | | | | | | |
| **Identify** **the document(s)** reviewed to verify the data is not retained after authorization. |  | | | | | |
| **Describe how** system configurations verified that the data is not retained after authorization. |  | | | | | |
| **3.2.d** For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable. | **Identify** **the document(s)** reviewed to verify that it defines processes for securely deleting the data so that it is unrecoverable. |  | | | | | |
| **Describe how** the processes for securely deleting the data were examined to verify that the data is unrecoverable. |  | | | | | |
| **3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.  **Note:** In the normal course of business, the following data elements from the magnetic stripe may need to be retained:   * The cardholder’s name * Primary account number (PAN) * Expiration date * Service code   To minimize risk, store only these data elements as needed for business. | | |  | ☐ | ☐ | ☐ | ☐ |
| **3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | **Identify the sample** of system components selected for 3.2.1-3.2.3. |  | | | | | |
| *For each data source type below from the sample of system of components examined,* **summarize the specific examples of each data source type observed** to verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | |
| * Incoming transaction data |  | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | |
| * History files |  | | | | | |
| * Trace files |  | | | | | |
| * Database schemas |  | | | | | |
| * Database contents |  | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | |
| **3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization. | | |  | ☐ | ☐ | ☐ | ☐ |
| **3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | |
| * Incoming transaction data |  | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | |
| * History files |  | | | | | |
| * Trace files |  | | | | | |
| * Database schemas |  | | | | | |
| * Database contents |  | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. | | |  | ☐ | ☐ | ☐ | ☐ |
| **3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that PINs and encrypted PIN blocks are not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | |
| * Incoming transaction data |  | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | |
| * History files |  | | | | | |
| * Trace files |  | | | | | |
| * Database schemas |  | | | | | |
| * Database contents |  | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN.  **Note:** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.3.a** Examine written policies and procedures for masking the display of PANs to verify:   * A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. * PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. * All roles not specifically authorized to see the full PAN must only see masked PANs. | **Identify the document(s)** reviewed to verify that written policies and procedures for masking the displays of PANs include the following:   * A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. * PAN must be masked when displayed such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN. * All roles not specifically authorized to see the full PAN must only see masked PANs. |  | | | | | |
| **3.3.b** Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests. | **Describe how** system configurations verified that: | | | | | | |
| * Full PAN is only displayed for users/roles with a documented business need. |  | | | | | |
| * PAN is masked for all other requests. |  | | | | | |
| **3.3.c** Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see more than first six/last four digits of the PAN. | **Describe how** displays of PAN verified that: | | | | | | |
| * PANs are masked when displaying cardholder data. |  | | | | | |
| * Only those with a legitimate business need are able to see more than first six/last four digits of the PAN. |  | | | | | |
| **3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:   * One-way hashes based on strong cryptography, (hash must be of the entire PAN). * Truncation (hashing cannot be used to replace the truncated segment of PAN). * Index tokens and pads (pads must be securely stored). * Strong cryptography with associated key-management processes and procedures.   **Note:** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity’s environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures | **Identify** **the documentation** examined to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  | | | | | |
| **3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). | **Identify** **the sample** of data repositories selected for this testing procedure. |  | | | | | |
| **Identify** **the tables or files** examined for each item in the sample of data repositories. |  | | | | | |
| *For each item in the sample*, **describe how** the tables or files verified that the PAN is rendered unreadable. |  | | | | | |
| **3.4.c** Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable. | **Identify the sample** of removable media selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** the sample of removable media confirmed that the PAN is rendered unreadable. |  | | | | | |
| **3.4.d** Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs. | **Identify the sample** of audit logs, including payment application logs, selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** the sample of audit logs, including payment application logs, confirmed that the PAN is rendered unreadable or is not present in the logs. |  | | | | | |
| **3.4.e** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | **Identify whether** hashed and truncated versions of the same PAN are present in the environment **(yes/no)**  *If ‘no,’* mark 3.4.e as ‘not applicable’ and proceed to 3.4.1. |  | | | | | |
| *If ‘yes,’* **describe** the implemented controls examined to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. |  | | | | | |
| **3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.  *Note: This requirement applies in addition to all other PCI DSS encryption and key management requirements.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.4.1.a** If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system’s authentication mechanism (for example, not using local user account databases or general network login credentials). | **Indicate whether** disk encryption is used. **(yes/no)** |  | | | | | |
| *If “yes,” complete the remainder of 3.4.1.a, 3.4.1.b, and 3.4.1.c.*  *If “no,” mark the remainder of 3.4.1.a, 3.4.1.b and 3.4.1.c as “Not Applicable.’* | | | | | | |
| **Describe** the disk encryption mechanism(s) in use. |  | | | | | |
| *For each disk encryption mechanism in use,* **describe how** the configuration verified that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  | | | | | |
| *For each disk encryption mechanism in use*, **describe how** the authentication process was observed to verify that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  | | | | | |
| **3.4.1.b** Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls). | **Describe how** processes were observed to verify that cryptographic keys are stored securely. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that cryptographic keys are stored securely. |  | | | | | |
| **3.4.1.c** Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored.  **Note:** If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method. | **Describe how** the configurations verified that cardholder data on removable media is encrypted wherever stored. |  | | | | | |
| **Describe how** processes were observed to verify that cardholder data on removable media is encrypted wherever stored. |  | | | | | |
| **3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:  **Note:** This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. | **Identify** **the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. |  | | | | | |
| **3.5.1 *Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes:   * Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date * Description of the key usage for each key. * Inventory of any HSMs and other SCDs used for key management | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.1** Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including:   * Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date * Description of the key usage for each key * Inventory of any HSMs and other SCDs used for key management | **Identify the responsible personnel interviewed** who confirm that a document exists to describe the cryptographic architecture, including:   * Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date * Description of the key usage for each key * Inventory of any HSMs and other SCDs used for key management |  | | | | | |
| **Identify the documentation reviewed** to verify thatit contains a description of the cryptographic architecture, including:   * Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date * Description of the key usage for each key * Inventory of any HSMs and other SCDs used for key management |  | | | | | |
| **3.5.2** Restrict access to cryptographic keys to the fewest number of custodians necessary. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.2** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary. | **Identify** **user access lists** examined. |  | | | | | |
| **Describe how** the user access lists verified that access to keys is restricted to the fewest number of custodians necessary. |  | | | | | |
| **3.5.3** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). * As at least two full-length key components or key shares, in accordance with an industry-accepted method.   **Note:** It is not required that public keys be stored in one of these forms. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.3.a** Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. | **Identify** **the documented procedures** examined to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. |  | | | | | |
| **3.5.3.b** Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one, (or more), of the following form at all times.   * Encrypted with a key-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. | **Provide the name** **of the assessor** who attests that all locations where keys are stored were identified. |  | | | | | |
| **Describe how** system configurations and key storage locations verified that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). * As key components or key shares, in accordance with an industry-accepted method. |  | | | | | |
| **3.5.3.c** Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify:   * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. | **Describe how** system configurations and key storage locations verified that, wherever key-encrypting keys are used: | | | | | | |
| * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. |  | | | | | |
| * Key-encrypting keys are stored separately from data-encrypting keys. |  | | | | | |
| **3.5.4** Store cryptographic keys in the fewest possible locations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.5.4** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations. | **Describe how** key storage locations and the observed processes verified that keys are stored in the fewest possible locations. |  | | | | | |
| **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:  **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.a *Additional Procedure for service provider assessments only***: If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. | **Indicate whether** the assessed entity is a service provider that shares keys with their customers for transmission or storage of cardholder data. **(yes/no)** |  | | | | | |
| *If “yes,”* **Identify** **the document** that the service provider provides to their customers examined to verify that it includes guidance on how to securely transmit, store and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. |  | | | | | |
| **3.6.b** Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following: | | | | | | | |
| **3.6.1** Generation of strong cryptographic keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.1.a** Verify that key-management procedures specify how to generate strong keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to generate strong keys. |  | | | | | |
| **3.6.1.b** Observe the procedures for generating keys to verify that strong keys are generated. | **Describe how** the procedures for generating keys were observed to verify that strong keys are generated. |  | | | | | |
| **3.6.2** Secure cryptographic key distribution. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.2.a** Verify that key-management procedures specify how to securely distribute keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to securely distribute keys. |  | | | | | |
| **3.6.2.b** Observe the method for distributing keys to verify that keys are distributed securely. | **Describe how** the method for distributing keys was observed to verify that keys are distributed securely. |  | | | | | |
| **3.6.3** Secure cryptographic key storage. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.3.a** Verify that key-management procedures specify how to securely store keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to securely store keys. |  | | | | | |
| **3.6.3.b** Observe the method for storing keys to verify that keys are stored securely. | **Describe how** the method for storing keys was observed to verify that keys are stored securely. |  | | | | | |
| **3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.4.a** Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). | **Identify** **the documented key-management procedures** examined to verify procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). |  | | | | | |
| **3.6.4.b** Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s). | **Identify** the responsible **personnel interviewed** who confirm that keys are changed at the end of the defined cryptoperiod(s). |  | | | | | |
| **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.  **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.5.a** Verify that key-management procedures specify processes for the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the documented key-management procedures** examined to verify that key-management processes specify the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | |
| **3.6.5.b** Interview personnel to verify the following processes are implemented:   * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. * Keys are replaced if known or suspected to be compromised. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the responsible personnel** interviewed who confirm that the following processes are implemented:   * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. * Keys are replaced if known or suspected to be compromised. * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | |
| **3.6.6** If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.  ***Note:*** Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.6.a** Verify that manual clear-text key-management procedures specify processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another. | **Indicate** **whether** manual clear-text cryptographic key-management operations are used. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 3.6.6.a and 3.6.6.b as “Not Applicable.”*  *If “yes,” complete 3.6.6.a and 3.6.6.b.* | | | | | | |
| **Identify the documented key-management procedures** examined to verify that manual clear-text key-management procedures define processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials of another. |  | | | | | |
| **3.6.6.b** Interview personnel and/or observe processes to verify that manual clear-text keys are managed with:   * Split knowledge, AND * Dual control | **Identify** **the responsible personnel** interviewed for this testing procedure, if applicable. |  | | | | | |
| For the interview, **summarize the relevant details discussed and/or describe how** processeswere observed to verify that manual clear-text keys are managed with: | | | | | | |
| * Split knowledge |  | | | | | |
| * Dual Control |  | | | | | |
| **3.6.7** Prevention of unauthorized substitution of cryptographic keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.7.a** Verify that key-management procedures specify processes to prevent unauthorized substitution of keys. | **Identify** **the documented key-management procedures** examined to verify that key-management procedures specify processes to prevent unauthorized substitution of keys. |  | | | | | |
| **3.6.7.b** Interview personnel and/or observe process to verify that unauthorized substitution of keys is prevented. | **Identify** **the responsible personnel** interviewed for this testing procedure, if applicable. |  | | | | | |
| For the interview, **summarize the relevant details discussed** **and/or describe how** processes were observed to verify that unauthorized substitution of keys is prevented. |  | | | | | |
| **3.6.8** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.8.a** Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Identify** **the documented key-management procedures** examined to verify that key-management procedures specify processes for key custodians to acknowledge that they understand and accept their key-custodian responsibilities. |  | | | | | |
| **3.6.8.b** Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Describe how** key custodian acknowledgements or other evidence were observed to verify that key custodians have acknowledged that they understand and accept their key-custodian responsibilities. |  | | | | | |
| **3.7** Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.7** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are:   * Documented, * In use, and * Known to all affected parties | **Identify** **the document** reviewed to verify that security policies and operational procedures for protecting stored cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting stored cardholder data are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 4: Encrypt transmission of cardholder data across open, public networks

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:   * Only trusted keys and certificates are accepted. * The protocol in use only supports secure versions or configurations. * The encryption strength is appropriat*e* for the encryption methodology in use.   *Examples of open, public networks include but are not limited to:*   * *The Internet* * *Wireless technologies, including 802.11 and Bluetooth* * *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* * *General Packet Radio Service (GPRS)* * *Satellite communications* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. | **Identify** all locations where cardholder data is transmitted or received over open, public networks. |  | | | | | |
| **Identify** **the documented standards** examined. |  | | | | | |
| **Describe how** the documented standards and system configurations both verified the use of: | | | | | | |
| * Security protocols for all locations |  | | | | | |
| * Strong cryptography for all locations |  | | | | | |
| **4.1.b** Review documented policies and procedures to verify processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. | **Identify the document** reviewed to verify that processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. |  | | | | | |
| **4.1.c** Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit. | **Describe** **the sample** of inbound and outbound transmissions that were observed as they occurred. |  | | | | | |
| **Describe how** the sample of inbound and outbound transmissions verified that all cardholder data is encrypted with strong cryptography during transit. |  | | | | | |
| **4.1.d** Examine keys and certificates to verify that only trusted keys and/or certificates are accepted. | *For all instances where cardholder data is transmitted or received over open, public networks:* | | | | | | |
| **Describe the mechanisms** used to ensure that only trusted keys and/or certificates are accepted. |  | | | | | |
| **Describe how** the mechanisms were observed to accept only trusted keys and/or certificates. |  | | | | | |
| **4.1.e** Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. | *For all instances where cardholder data Is transmitted or received over open, public networks,* **describe how** system configurations verified that the protocol: | | | | | | |
| * Is implemented to use only secure configurations. |  | | | | | |
| * Does not support insecure versions or configurations. |  | | | | | |
| **4.1.f** Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) | *For each encryption methodology in use,* | | | | | | |
| **Identify** vendor recommendations/best practices for encryption strength. |  | | | | | |
| **Identify** the encryption strength observed to be implemented. |  | | | | | |
| **4.1.g** For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.  *For example, for browser-based implementations:*   * *“HTTPS” appears as the browser Universal Record Locator (URL) protocol; and* * *Cardholder data is only requested if “HTTPS” appears as part of the URL.* | **Indicate whether** TLS is implemented to encrypt cardholder data over open, public networks. **(yes/no)**  *If ‘no,’ mark the remainder of 4.1.g as ‘not applicable.’* |  | | | | | |
| *If “yes,” for all instances where TLS is used to encrypt cardholder data over open, public networks,***describe how** system configurations verified that TLS is enabled whenever cardholder data is transmitted or received. |  | | | | | |
| **4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.1** Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified:   * Industry best practices are used to implement strong encryption for authentication and transmission. * Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission. | **Identify** all wireless networks transmitting cardholder data or connected to the cardholder data environment. |  | | | | | |
| **Identify the documented standards** examined. |  | | | | | |
| **Describe how** the documented standards and system configuration settings both verified the following for all wireless networks identified: | | | | | | |
| * Industry best practices are used to implement strong encryption for authentication and transmission. |  | | | | | |
| * Weak encryption is not used as a security control for authentication or transmission. |  | | | | | |
| **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | **Indicate** **whether** end-user messaging technologies are used to send cardholder data. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 4.2.a as “Not Applicable” and proceed to 4.2.b.*  *If “yes,” complete the following:* | | | | | | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **Describe** **the sample** of outbound transmissions that were observed as they occurred. |  | | | | | |
| **Describe how** the sample of outbound transmissions verified that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **4.2.b** Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. | **Identify** **the policy document** that prohibits PAN from being sent via end-user messaging technologies under any circumstances. |  | | | | | |
| **4.3** Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.3** Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for encrypting transmissions of cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for encrypting transmissions of cardholder data are:   * In use * Known to all affected parties |  | | | | | |

### Maintain a Vulnerability Management Program

#### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  | | | | | |
| **5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | **Identify** **the vendor documentation** reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  | | | | | |
| **Describe how** anti-virus configurations verified that anti-virus programs: | | | | | | |
| * Detect all known types of malicious software, |  | | | | | |
| * Remove all known types of malicious software, and |  | | | | | |
| * Protect against all known types of malicious software. |  | | | | | |
| **5.1.2** For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.1.2** Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software. | **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, and that such systems continue to not require anti-virus software. |  | | | | | |
| **5.2** Ensure that all anti-virus mechanisms are maintained as follows:   * Are kept current. * Perform periodic scans. * Generate audit logs which are retained per PCI DSS Requirement 10.7. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.2.a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up-to-date. | **Identify** **the documented policies and procedures** examined to verify that anti-virus software and definitions are required to be kept up to date. |  | | | | | |
| **5.2.b** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are:   * Configured to perform automatic updates, and * Configured to perform periodic scans. | **Describe how** anti-virus configurations, including the master installation of the software, verified anti-virus mechanisms are: | | | | | | |
| * Configured to perform automatic updates, and |  | | | | | |
| * Configured to perform periodic scans. |  | | | | | |
| **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:   * The anti-virus software and definitions are current. * Periodic scans are performed. | **Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure. |  | | | | | |
| **Describe how** the system components verified that: | | | | | | |
| * The anti-virus software and definitions are current. |  | | | | | |
| * Periodic scans are performed. |  | | | | | |
| **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:   * Anti-virus software log generation is enabled, and * Logs are retained in accordance with PCI DSS Requirement 10.7. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, verified that: | | | | | | |
| * Anti-virus software log generation is enabled, and. |  | | | | | |
| * Logs are retained in accordance with PCI DSS Requirement 10.7. |  | | | | | |
| **5.3** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.  **Note:** Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.3.a** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software is actively running. |  | | | | | |
| **5.3.b** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users. | *For each item in the sample from 5.3.a,* **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software cannot be disabled or altered by users. |  | | | | | |
| **5.3.c** Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. | **Identify** **the responsible personnel** interviewed who confirm that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | |
| **Describe how** processes were observed to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | |
| **5.4** Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.4** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for protecting systems against malware are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting systems against malware are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 6: Develop and maintain secure systems and applications

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.  **Note:** Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.  Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.1.a** Examine policies and procedures to verify that processes are defined for the following:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. | **Identify** **the documented policies and procedures** examined to confirm that processes are defined:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. |  | | | | | |
| **6.1.b** Interview responsible personnel and observe processes to verify that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. | **Identify the responsible personnel** interviewed who confirm that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | |
| **Describe how** processes were observed to verify that: | | | | | | |
| * New security vulnerabilities are identified. |  | | | | | |
| * A risk ranking is assigned to vulnerabilities to include identification of all “high” risk and “critical” vulnerabilities. |  | | | | | |
| * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | |
| **Identify** the outside sources used. |  | | | | | |
| **6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.  **Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.2.a** Examine policies and procedures related to security-patch installation to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months). | **Identify** **the documented policies and procedures** related to security-patch installation examined to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame. |  | | | | | |
| **6.2.b** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:   * That applicable critical vendor-supplied security patches are installed within one month of release. * All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). | **Identify** **the sample** of system components and related software selected for this testing procedure. |  | | | | | |
| **Identify** **the vendor security patch list** reviewed. |  | | | | | |
| *For each item in the sample,* **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify that: | | | | | | |
| * Applicable critical vendor-supplied security patches are installed within one month of release. |  | | | | | |
| * All applicable vendor-supplied security patches are installed within an appropriate time frame. |  | | | | | |
| **6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:   * In accordance with PCI DSS (for example, secure authentication and logging). * Based on industry standards and/or best practices. * Incorporate information security throughout the software development life cycle.   **Note**: this applies to all software developed internally as well as bespoke or custom software developed by a third party. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.3.a** Examine written software-development processes to verify that the processes are based on industry standards and/or best practices. | **Identify** **the document** examined to verify that software-development processes are based on industry standards and/or best practices. |  | | | | | |
| **6.3.b** Examine written software-development processes to verify that information security is included throughout the life cycle. | **Identify** **the documented software-development processes** examined to verify that information security is included throughout the life cycle. |  | | | | | |
| **6.3.c** Examine written software-development processes to verify that software applications are developed in accordance with PCI DSS. | **Identify** **the documented software-development processes** examined to verify that software applications are developed in accordance with PCI DSS. |  | | | | | |
| **6.3.d** Interview software developers to verify that written software development processes are implemented. | **Identify** **the software developers** interviewed who confirm that written software-development processes are implemented. |  | | | | | |
| **6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.3.1** Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. | **Identify** **the documented software-development processes** examined to verify processes define that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | |
| **6.3.2** Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:   * Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines. * Appropriate corrections are implemented prior to release. * Code review results are reviewed and approved by management prior to release.   **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.  *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.3.2.a** Examine written software development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. | **Identify** **the documented software-development processes** examined to verify processes define that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | |
| **6.3.2.b** Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above. | **Identify** **the sample** of recent custom application changes selected for this testing procedure. |  | | | | | |
| *For each item in the sample*, **describe how** code review processes were observed to verify custom application code is reviewed as follows: | | | | | | |
| * Code changes are reviewed by individuals other than the originating code author. |  | | | | | |
| * Code changes are reviewed by individuals who are knowledgeable in code-review techniques and secure coding practices. |  | | | | | |
| * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). |  | | | | | |
| * Appropriate corrections are implemented prior to release. |  | | | | | |
| * Code-review results are reviewed and approved by management prior to release. |  | | | | | |
| **6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4** Examine policies and procedures to verify the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change control procedures related to implementing security patches and software modifications are documented. | **Identify the documented policies and procedures** examined to verify that the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change-control procedures related to implementing security patches and software modifications are documented. |  | | | | | |
| **6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.1.a** Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s). | **Identify the network documentation** examined to verify that the development/test environments are separate from the production environment(s). |  | | | | | |
| **Describe how** network device configurations verified that the development/test environments are separate from the production environment(s). |  | | | | | |
| **6.4.1.b** Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s). | **Identify the access control settings** examined for this testing procedure. |  | | | | | |
| **Describe how** the access control settings verified that access controls are in place to enforce separation between the development/test environments and the production environment(s). |  | | | | | |
| **6.4.2** Separation of duties between development/test and production environments. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.2** Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment. | **Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | |
| **Identify the personnel assigned to production environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | |
| **Describe how** processes were observed to verify that separation of duties is in place between development/test environments and the production environment. |  | | | | | |
| **6.4.3** Production data (live PANs) are not used for testing or development. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development. | **Identify the responsible personnel** interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development. |  | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing. |  | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development. |  | | | | | |
| **6.4.3.b** Examine a sample of test data to verify production data (live PANs) is not used for testing or development. | **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for testing. |  | | | | | |
| **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for development. |  | | | | | |
| **6.4.4** Removal of test data and accounts from system components before the system becomes active / goes into production. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.4.a** Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active. | **Identify the responsible personnel** interviewed who confirm that test data and accounts are removed before a production system becomes active. |  | | | | | |
| **Describe how** testing processes were observed to verify that test data is removed before a production system becomes active. |  | | | | | |
| **Describe how** testing processes were observed to verify that test accounts are removed before a production system becomes active. |  | | | | | |
| **6.4.4.b** Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active. | **Describe how** the sampled data examined verified that test data is removed before the system becomes active. |  | | | | | |
| **Describe how** the sampled data examined verified that test accounts are removed before the system becomes active. |  | | | | | |
| **6.4.5** Change control procedures must include the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.a** Examine documented change-control procedures and verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. | **Identify** **the documented change-control procedures** examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  | | | | | |
| **6.4.5.b** For a sample of system components, interview responsible personnel to determine recent changes. Trace those changes back to related change control documentation. For each change examined, perform the following: | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| **Identify the responsible personnel** interviewed to determine recent changes. |  | | | | | |
| *For each item in the sample,* **identify** **the sample** of changes and the related change control documentation selected for this testing procedure (through 6.4.5.4). |  | | | | | |
| **6.4.5.1** Documentation of impact. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change. | *For each change from 6.4.5.b*, **describe how** the documentation of impact is included in the change control documentation for each sampled change. |  | | | | | |
| **6.4.5.2** Documented change approval by authorized parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change. | *For each change from 6.4.5.b*, **describe how** documented approval by authorized parties is present in the change control documentation for each sampled change. |  | | | | | |
| **6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. | *For each change from 6.4.5.b*, **describe how** the change control documentation confirmed that functionality testing is performed to verify that the change does not adversely impact the security of the system. |  | | | | | |
| **6.4.5.3.b** For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **identify** **the sample** of custom code changes and the related change control documentation selected for this testing procedure. |  | | | | | |
| For each change, **describe how** the change control documentation verified that updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. |  | | | | | |
| **6.4.5.4** Back-out procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.5.4** Verify that back-out procedures are prepared for each sampled change. | *For each change from 6.4.5.b*, **describe how** the change control documentation verified that back-out procedures are prepared. |  | | | | | |
| **6.4.6** Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.4.6** For a sample of significant changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change. | **Identify whether** a significant change occurred within the past 12 months. **(yes/no)**  *If “yes,” complete the following:*  *If “no,” mark the rest of 6.4.6 as “Not Applicable”* |  | | | | | |
| **Identify the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| **Identify the relevant documentation** reviewed to verify that the documentation was updated as part of the change. |  | | | | | |
| **Identify the sample of change records** examined for this testing procedure. |  | | | | | |
| **Identify the sample of systems/networks** affected by the significant change. |  | | | | | |
| *For each sampled change,* **describe how**the system/networks observed verified that applicable PCI DSS requirements were implemented and documentation updated as part of the change. | | | | | | |
|  | | | | | | |
| **6.5** Address common coding vulnerabilities in software-development processes as follows:   * Traindevelopers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. * Develop applications based on secure coding guidelines.   **Note:** The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.a** Examine software development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers at least annually, based on industry best practices and guidance. | **Identify** **the document** reviewed to verify that up-to-date training in secure coding techniques is required for developers at least annually. |  | | | | | |
| **Identify** the industry best practices and guidance on which the training is based. |  | | | | | |
| **6.5.b** Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities | **Identify the records** **of training** that were examined to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities. |  | | | | | |
| **6.5.c** Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: | **Identify** **the software-development policies and procedures** examined to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10. |  | | | | | |
| **Identify** **the responsible personnel** interviewed to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10. |  | | | | | |
| **Note:** Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external): | | | | | | | |
| **6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.1** Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include:   * Validating input to verify user data cannot modify meaning of commands and queries. * Utilizing parameterized queries. | *For the interviews at 6.5.c***, summarize the relevant details** discussed to verify that injection flaws are addressed by coding techniques that include: | | | | | | |
| * Validating input to verify user data cannot modify meaning of commands and queries. |  | | | | | |
| * Utilizing parameterized queries. |  | | | | | |
| **6.5.2** Buffer overflow. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.2** Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include:   * Validating buffer boundaries. * Truncating input strings. | *For the interviews at 6.5.c***, summarize the relevant details** discussed to verify that buffer overflows are addressed by coding techniques that include: | | | | | | |
| * Validating buffer boundaries. |  | | | | | |
| * Truncating input strings. |  | | | | | |
| **6.5.3** Insecure cryptographic storage. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.3** Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that:   * Prevent cryptographic flaws. * Use strong cryptographic algorithms and keys. | *For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that insecure cryptographic storage is addressed by coding techniques that: | | | | | | |
| * Prevent cryptographic flaws. |  | | | | | |
| * Use strong cryptographic algorithms and keys. |  | | | | | |
| **6.5.4** Insecure communications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.4** Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications. | *For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that insecure communications are addressed by coding techniques that properly: | | | | | | |
| * Authenticate all sensitive communications. |  | | | | | |
| * Encrypt all sensitive communications. |  | | | | | |
| **6.5.5** Improper error handling. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.5** Examine software-development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages(for example, by returning generic rather than specific error details). | *For the interviews at 6.5.c***, summarize the relevant details** discussed to verify that improper error handling is addressed by coding techniques that do not leak information via error messages. |  | | | | | |
| **6.5.6** All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.6** Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1. | *For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1. |  | | | | | |
| **Note:** Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external): | | | | | | | |
| **Indicate** **whether** web applications and application interfaces are present. **(yes/no)**  *If “no,”* mark the below 6.5.7-6.5.10 as “Not Applicable.”  *If “yes,”* ***complete the following:*** | |  | | | | | |
| **6.5.7** Cross-site scripting (XSS). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.7** Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include:   * Validating all parameters before inclusion. * Utilizing context-sensitive escaping. | *For the interviews at 6.5.c***, summarize the relevant details** discussed to verify that cross-site scripting (XSS) is addressed by coding techniques that include: | | | | | | |
| * Validating all parameters before inclusion. |  | | | | | |
| * Utilizing context-sensitive escaping. |  | | | | | |
| **6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.8** Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that include:   * Proper authentication of users. * Sanitizing input. * Not exposing internal object references to users. * User interfaces that do not permit access to unauthorized functions. | *For the interviews at 6.5.c***, summarize the relevant details** discussed to verify that improper access control is addressed by coding techniques that include: | | | | | | |
| * Proper authentication of users. |  | | | | | |
| * Sanitizing input. |  | | | | | |
| * Not exposing internal object references to users. |  | | | | | |
| * User interfaces that do not permit access to unauthorized functions. |  | | | | | |
| **6.5.9** Cross-site request forgery (CSRF). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.9** Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. | *For the interviews at 6.5.c***, summarize the relevant details** discussed to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. |  | | | | | |
| **6.5.10** Broken authentication and session management**.** | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.10** Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include:   * Flagging session tokens (for example, cookies) as “secure.” * Not exposing session IDs in the URL. * Incorporating appropriate time-outs and rotation of session IDs after a successful login. | *For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that broken authentication and session management are addressed via coding techniques that commonly include: | | | | | | |
| * Flagging session tokens (for example, cookies) as “secure.” |  | | | | | |
| * Not exposing session IDs in the URL. |  | | | | | |
| * Incorporating appropriate time-outs and rotation of session IDs after a successful login. |  | | | | | |
| **6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:   * Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.   **Note:** This assessment is not the same as the vulnerability scans performed for Requirement 11.2.   * Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.6** For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows:   * Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. * Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. | For each public-facing web application, **identify which** of the two methods are implemented:   * Web application vulnerability security assessments, AND/OR * Automated technical solution that detects and prevents web-based attacks, such as web application firewalls. |  | | | | | |
| *If application vulnerability security assessments are indicated above:* | | | | | | |
| **Describe the tools and/or methods** used (manual or automated, or a combination of both). |  | | | | | |
| **Identify the documented processes** that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected * That the application is re-evaluated after the corrections. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that public-facing web applications are reviewed, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. |  | | | | | |
| **Identify the records of application vulnerability security assessments** examined for this testing procedure. |  | | | | | |
| **Describe how** the records of application vulnerability security assessments verified that public-facing web applications are reviewed as follows: | | | | | | |
| * At least annually. |  | | | | | |
| * After any changes. |  | | | | | |
| * By an organization that specialized in application security. |  | | | | | |
| * That at a minimum, all vulnerabilities in requirement 6.5 are included in the assessment. |  | | | | | |
| * That all vulnerabilities are corrected. |  | | | | | |
| * That the application is re-evaluated after the corrections. |  | | | | | |
| *If an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is indicated above:* | | | | | | |
| **Describe** the automated technical solution in use that detects and prevents web-based attacks. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above automated technical solution is in place as follows:   * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | |
| **Describe how** the system configuration settings verified that the above automated technical solution is in place as follows: | | | | | | |
| * Is situated in front of public-facing web applications to detect and prevent web-based attacks. |  | | | | | |
| * Is actively running and up-to-date as applicable. |  | | | | | |
| * Is generating audit logs. |  | | | | | |
| * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | |
| **6.7** Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.7** Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** examined to verify that security policies and operational procedures for developing and maintaining secure systems and applications are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for developing and maintaining secure systems and applications are:   * In use * Known to all affected parties |  | | | | | |

### Implement Strong Access Control Measures

#### Requirement 7: Restrict access to cardholder data by business need to know

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.a** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function. * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  | | | | | |
| **7.1.1** Define access needs for each role, including:   * System components and data resources that each role needs to access for their job function. * Level of privilege required (for example, user, administrator, etc.) for accessing resources. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.1** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | **Identify** **the selected sample** of roles for this testing procedure. |  | | | | | |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs are defined and include: | | | | | | |
| * System components and data resources that each role needs to access for their job function. |  | | | | | |
| * Identification of privilege necessary for each role to perform their job function. |  | | | | | |
| **7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.2.a** Interview personnel responsible for assigning access to verify that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.2.b** Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the sample** of user IDs ***with privileged access*** selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed to confirm that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are: | | | | | | |
| * Necessary for that individual’s job function. |  | | | | | |
| * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.3** Assign access based on individual personnel’s job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.3** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. | **Identify the sample** of user IDs selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed who confirm that privileges assigned are based on that individual’s job classification and function. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are based on that individual’s job classification and function. |  | | | | | |
| **7.1.4** Require documented approval by authorized parties specifying required privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.4** Select a sample of user IDs and compare with documented approvals to verify that:   * Documented approval exists for the assigned privileges. * The approval was by authorized parties. * That specified privileges match the roles assigned to the individual. | **Identify the sample** of user IDs selected for this testing procedure. |  | | | | | |
| For each user ID in the selected sample, **describe how**: | | | | | | |
| * Documented approval exists for the assigned privileges. |  | | | | | |
| * The approval was by authorized parties. |  | | | | | |
| * That specified privileges match the roles assigned to the individual. |  | | | | | |
| **7.2** Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.  This access control system(s) must include the following: | | | | | | | |
| **7.2** Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows: | | | | | | | |
| **7.2.1** Coverage of all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.1** Confirm that access control systems are in place on all system components. | **Identify** **vendor documentation** examined. |  | | | | | |
| **Describe how** system settings and the vendor documentation verified that access control systems are in place on all system components. |  | | | | | |
| **7.2.2** Assignment of privileges to individuals based on job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | **Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  | | | | | |
| **7.2.3** Default “deny-all” setting. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.3** Confirm that the access control systems have a default “deny-all” setting. | **Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems have a default “deny-all” setting. |  | | | | | |
| **7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.3** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting access to cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for restricting access to cardholder data are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 8: Identify and authenticate access to system components

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.a** Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8:   * Assign all users a unique ID before allowing them to access system components or cardholder data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   Enabled only during the time period needed and disabled when not in use.  Monitored when in use.   * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  | | | | | |
| **8.1.b** Verify that procedures are implemented for user identification management, by performing the following: | | | | | | | |
| **8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.1** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data. | **Identify** **the responsible administrative personnel** interviewed who confirm that all users are assigned a unique ID for access to system components or cardholder data. |  | | | | | |
| **8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.2** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval. | **Identify** **the sample** of privileged user IDs selected for this testing procedure. |  | | | | | |
| **Identify** **the sample** of general user IDs selected for this testing procedure. |  | | | | | |
| **Describe how** observed system settings and the associated authorizations verified that each ID has been implemented with only the privileges specified on the documented approval: | | | | | | |
| * For the sample of privileged user IDs. |  | | | | | |
| * For the sample of general user IDs. |  | | | | | |
| **8.1.3** Immediately revoke access for any terminated users. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.3.a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** **the sample** of users terminated in the past six months that were selected for this testing procedure. |  | | | | | |
| **Describe how** the current user access lists for ***local access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **Describe how** the current user access lists for ***remote access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **8.1.3.b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  | | | | | |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  | | | | | |
| **8.1.4** Remove/disable inactive user accounts within 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. | **Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled. |  | | | | | |
| **8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:   * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.5.a** Interview personnel and observe processes for managing accounts used by third parties to access, support, or maintain system components to verify that accounts used for remote access are:   * Disabled when not in use. * Enabled only when needed by the third party, and disabled when not in use. | **Identify** **the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are:   * Disabled when not in use. * Enabled only when needed by the third party, and disabled when not in use. |  | | | | | |
| **Describe how** processes for managing third party accounts were observed to verify that accounts used for remote access are: | | | | | | |
| * Disabled when not in use. |  | | | | | |
| * Enabled only when needed by the third party, and disabled when not in use. |  | | | | | |
| **8.1.5.b** Interview personnel and observe processes to verify that third party remote access accounts are monitored while being used. | **Identify** **the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are monitored while being used. |  | | | | | |
| **Describe how** processes for managing third party remote access were observed to verify that accounts are monitored while being used. |  | | | | | |
| **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that authentication parameters are set to require that user accounts be locked after not more than six invalid logon attempts. |  | | | | | |
| **8.1.6.b** ***Additional procedure for service provider assessments only:*** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **Describe how** implemented processes were observed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. |  | | | | | |
| **8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that system/session idle time out features have been set to 15 minutes or less. |  | | | | | |
| **8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:   * Something you know, such as a password or passphrase. * Something you have, such as a token device or smart card. * Something you are, such as a biometric. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following:   * Examine documentation describing the authentication method(s) used. * For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s). | **Identify the document** describing the authentication method(s) used that was reviewed to verify that the methods require users to be authenticated using a unique ID and additional authentication for access to the cardholder data environment. |  | | | | | |
| **Describe** the authentication methods used (for example, a password or passphrase, a token device or smart card, a biometric, etc.) for each type of system component. |  | | | | | |
| *For each type of authentication method used and for each type of system component,* **describe how** the authentication method was observed to be functioning consistently with the documented authentication method(s). |  | | | | | |
| **8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.1.a** Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage. | **Identify** **the vendor documentation** examined to verify that passwords are protected with strong cryptography during transmission and storage. |  | | | | | |
| **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,***describe how** system configuration settings verified that passwords are protected with strong cryptography during ***transmission***. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that passwords are protected with strong cryptography during ***storage***. |  | | | | | |
| **8.2.1.b** For a sample of system components, examine password files to verify that passwords are unreadable during storage. | *For each item in the sample at 8.2.1.a,* **describe how** password files verified that passwords are unreadable during storage. |  | | | | | |
| **8.2.1.c** For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission. | *For each item in the sample at 8.2.1.a,* **describe how** data transmissions verified that passwords are unreadable during transmission. |  | | | | | |
| **8.2.1.d** ***Additional procedure for service provider assessments only:*** Observe password files to verify that non-consumer customer passwords are unreadable during storage. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during storage. |  | | | | | |
| **8.2.1.e *Additional procedure for service provider assessments only:*** Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during transmission. |  | | | | | |
| **8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.2** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. | **Identify the document** examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  | | | | | |
| **Describe** the non-face-to-face methods used for requesting password resets. |  | | | | | |
| For each non-face-to-face method, **describe how** security personnel were observed to verify the user’s identity before the authentication credential was modified. |  | | | | | |
| **8.2.3** Passwords/passphrases must meet the following:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters.   Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.3.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that user password/passphrase parameters are set to require at least the following strength/complexity: | | | | | | |
| * Require a minimum length of at least seven characters. |  | | | | | |
| * Contain both numeric and alphabetic characters. |  | | | | | |
| **8.2.3.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. | *Additional procedure for service provider assessments only:***Identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:   * A minimum length of at least seven characters. * Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters. |  | | | | | |
| **Describe how** internal processes were observed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: | | | | | | |
| * A minimum length of at least seven characters. |  | | | | | |
| * Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters. |  | | | | | |
| **8.2.4** Change user passwords/passphrases at least once every 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days. |  | | | | | |
| **8.2.4.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that:   * Non-consumer customer user passwords/passphrases are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that:   * Non-consumer customer user passwords/passphrases are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. |  | | | | | |
| **Describe how** internal processes were observed to verify that: | | | | | | |
| * Non-consumer customer user passwords/passphrases are required to change periodically; and |  | | | | | |
| * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. |  | | | | | |
| **8.2.5** Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password/passphrase parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings verified that password/passphrase parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. |  | | | | | |
| **8.2.5.b** ***Additional Procedure for service provider assessments only:*** Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. |  | | | | | |
| **Describe how** internal processes were observed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. |  | | | | | |
| **8.2.6** Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use. | **Identify** **the documented password procedures** examined to verify the procedures define that:   * First-time passwords/passphrases must be set to a unique value for each user. * First-time passwords/passphrases must be changed after the first use. * Reset passwords/passphrases must be set to a unique value for each user. * Reset passwords/passphrases must be changed after the first use. |  | | | | | |
| **Describe how** security personnel were observed to: | | | | | | |
| * Set first-time passwords/passphrases to a unique value for each new user. |  | | | | | |
| * Set first-time passwords/passphrases to be changed after first use. |  | | | | | |
| * Set reset passwords/passphrases to a unique value for each existing user. |  | | | | | |
| * Set reset passwords/passphrases to be changed after first use. |  | | | | | |
| **8.3** Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication  **Note:** Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. | | | | | | | |
| **8.3.1** Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.1.a** Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE. | **Identify the sample of network and/or system components** examined for this testing procedure. |  | | | | | |
| **Describe how** the configurations verify that multi-factor authentication is required for all non-console access into the CDE. | | | | | | |
|  | | | | | | |
| **8.3.1.b** Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used. | **Identify the sample of administrator personnel** observed logging in to the CDE. |  | | | | | |
| **Describe** the multi-factor authentication methods observed to be in place for administrator personnel non-console log ins to the CDE. | | | | | | |
|  | | | | | | |
| **8.3.2** Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity’s network. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.2.a** Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for:   * All remote access by personnel, both user and administrator, and * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). | **Describe how** system configurations for remote access servers and systems verified that multi-factor authentication is required for: | | | | | | |
| * All remote access by personnel, both user and administrator, and |  | | | | | |
| * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). |  | | | | | |
| **8.3.2.b** Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used. | **Identify the sample of personnel** observed connecting remotely to the network. |  | | | | | |
| *For each individual in the sample,* **describe how** multi-factor authentication was observed to be required for remote access to the network. |  | | | | | |
| **8.4** Document and communicate authentication policies and procedures to all users including:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.4.a** Examineprocedures and interview personnel to verify that authentication policies and procedures are distributed to all users. | **Identify** **the documented policies and procedures** examined to verify authentication procedures define that authentication procedures and policies are distributed to all users. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that authentication policies and procedures are distributed to all users. |  | | | | | |
| **8.4.b** Review authentication policies and procedures that are distributed to users and verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | **Identify the documented authentication policies and procedures that** **are distributed to users** reviewed to verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * That users should change passwords if there is any suspicion the password could be compromised. |  | | | | | |
| **8.4.c** Interview a sample of users to verify that they are familiar with authentication policies and procedures. | **Identify** **the sample** of users interviewed for this testing procedure. |  | | | | | |
| For each user in the sample, **summarize the relevant details** discussed that verify that they are familiar with authentication policies and procedures. |  | | | | | |
| **8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:   * Generic user IDs are disabled or removed. * Shared user IDs do not exist for system administration and other critical functions. * Shared and generic user IDs are not used to administer any system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.a** For a sample of system components, examine user ID lists to verify the following:   * Generic user IDs are disabled or removed. * Shared user IDs for system administration activities and other critical functions do not exist. * Shared and generic user IDs are not used to administer any system components. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** the user ID lists verified that: | | | | | | |
| * Generic user IDs are disabled or removed. |  | | | | | |
| * Shared user IDs for system administration activities and other critical functions do not exist. |  | | | | | |
| * Shared and generic user IDs are not used to administer any system components. |  | | | | | |
| **8.5.b** Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. | **Identify** **the documented policies and procedures** examined to verify authentication policies/procedures define that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. |  | | | | | |
| **8.5.c** Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. | **Identify** **the system administrators** interviewed who confirm that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. |  | | | | | |
| **8.5.1** ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.  This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.1** ***Additional procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer. | **Identify** **the documented procedures** examined to verify that different authentication credentials are used for access to each customer. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that different authentication credentials are used for access to each customer |  | | | | | |
| **8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows:   * Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.6.a** Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. | **Identify** **the documented authentication policies and procedures** examined to verify the procedures for using authentication mechanisms define that:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.6.b** Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts. | **Identify the security personnel** interviewed who confirm that authentication mechanisms are assigned to an account and not shared among multiple accounts. |  | | | | | |
| **8.6.c** Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings and/or physical controls, as applicable, verified that controls are implemented to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:   * All user access to, user queries of, and user actions on databases are through programmatic methods. * Only database administrators have the ability to directly access or query databases. * Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.7.a** Review database and application configuration settings and verify that all users are authenticated prior to access. | **Identify** all databases containing cardholder data. |  | | | | | |
| **Describe how** database and/or application configuration settings verified that all users are authenticated prior to access. |  | | | | | |
| **8.7.b** Examine database and application configuration settings to verify thatall user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). | *For each database from 8.7.a,* **describe how** the database and application configuration settings verified that all user access to, user queries of, and user actions on the database are through programmatic methods only. |  | | | | | |
| **8.7.c** Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators. | *For each database from 8.7.a*, **describe how** database application configuration settings verified that user direct access to or queries of databases are restricted to database administrators. |  | | | | | |
| **8.7.d** Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes). | *For each database from 8.7.a:* | | | | | | |
| **Identify** applications with access to the database. |  | | | | | |
| **Describe how** database access control settings, database application configuration settings and related application IDs verified that application IDs can only be used by the applications. |  | | | | | |
| **8.8** Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.8** Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for identification and authentication are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for identification and authentication are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 9: Restrict physical access to cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. * Observe a system administrator’s attempt to log into consoles for randomly selected systems in the cardholder data environment and verify that they are “locked” to prevent unauthorized use. | **Identify and briefly describe** all of the following with systems in the cardholder data environment: | | | | | | |
| * All computer rooms |  | | | | | |
| * All data centers |  | | | | | |
| * Any other physical areas |  | | | | | |
| *For each area identified (add rows as needed),* complete the following: | | | | | | |
| **Describe** the physical security controls observed to be in place, including authorized badges and lock and key. |  | | | | | |
| **Identify** the randomly selected systems in the cardholder environment for which a system administrator login attempt was observed. |  | | | | | |
| **Describe how** consoles for the randomly selected systems were observed to be “locked” when not in use. |  | | | | | |
| **9.1.1** Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.  **Note:** “Sensitive areas” refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1.1.a** Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas. | **Describe** either the video cameras or access control mechanisms (or both) observed to monitor the entry/exit points to sensitive areas. |  | | | | | |
| **9.1.1.b** Verify that either video cameras or access control mechanisms (or both) are protected from tampering or disabling. | **Describe how** either the video cameras or access control mechanisms (or both) were observed to be protected from tampering and/or disabling. |  | | | | | |
| **9.1.1.c** Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months. | **Describe how** the data from video cameras and/or access control mechanisms were observed to be reviewed. |  | | | | | |
| **Describe how** data was observed to be stored for at least three months. |  | | | | | |
| **9.1.2** Implement physical and/or logical controls to restrict access to publicly accessible network jacks.  For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks. | **Identify the responsible personnel** interviewed who confirm that physical and/or logical controls are in place to restrict access to publicly accessible network jacks. |  | | | | | |
| **Describe how** physical and/or logical controls were observed to be in place to restrict access to publicly accessible network jacks. |  | | | | | |
| **9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted. | **Describe how** physical access was observed to be restricted to the following: | | | | | | |
| * Wireless access points |  | | | | | |
| * Wireless gateways |  | | | | | |
| * Wireless handheld devices |  | | | | | |
| * Network/communications hardware |  | | | | | |
| * Telecommunication lines |  | | | | | |
| **9.2** Develop procedures to easily distinguish between onsite personnel and visitors, to include:   * Identifying onsite personnel and visitors (for example, assigning badges). * Changes to access requirements. * Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.2.a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | **Identify** **the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  | | | | | |
| **9.2.b** Examine identification methods (such as ID badges) andobserve processes for identifying and distinguishing between onsite personnel and visitors to verify that:   * Visitors are clearly identified, and * It is easy to distinguish between onsite personnel and visitors. | **Identify** the identification methods examined. |  | | | | | |
| **Describe how** processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that: | | | | | | |
| * Visitors are clearly identified, and |  | | | | | |
| * It is easy to distinguish between onsite personnel and visitors. |  | | | | | |
| **9.2.c** Verify that access to the identification process (such as a badge system) is limited to authorized personnel. | **Describe how** access to the identification process was observed to be limited to authorized personnel. |  | | | | | |
| **9.3** Control physical access for onsite personnel to sensitive areas as follows:   * Access must be authorized and based on individual job function. * Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.3.a** For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that:   * Access to the sensitive area is authorized. * Access is required for the individual’s job function. | **Identify the sample** of responsible personnel interviewed for this testing procedure. |  | | | | | |
| *For the interview,* **summarize the relevant details** discussed to verify that: | | | | | | |
| * Access to the sensitive area is authorized. |  | | | | | |
| * Access is required for the individual’s job function. |  | | | | | |
| **9.3.b** Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access. | **Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access. |  | | | | | |
| **9.3.c** Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas. | **Identify** **the sample** of users recently terminated. |  | | | | | |
| *For all items in the sample,* **provide the name of the assessor** who attests that the access control lists were reviewed to verify the personnel do not have physical access to sensitive areas. |  | | | | | |
| **9.4** Implement procedures to identify and authorize visitors.  Procedures should include the following: | | | | | | | |
| **9.4** Verify that visitor authorization and access controls are in place as follows: | | | | | | | |
| **9.4.1** Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.1.a** Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. | **Identify the documented procedures** examined to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. |  | | | | | |
| **9.4.1.b** Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. | **Describe how** the use of visitor badges or other identification was observed to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. |  | | | | | |
| **9.4.2** Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.2.a** Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel. | **Describe how** people within the facility were observed to use visitor badges or other identification. |  | | | | | |
| **Describe how** visitors within the facility were observed to be easily distinguishable from onsite personnel. |  | | | | | |
| **9.4.2.b** Verify that visitor badges or other identification expire. | **Describe how** visitor badges or other identification were verified to expire. |  | | | | | |
| **9.4.3** Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.3** Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration. | **Describe how** visitors leaving the facility were observed to verify they are asked to surrender their badge or other identification upon departure or expiration. |  | | | | | |
| **9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.  Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log.  Retain this log for a minimum of three months, unless otherwise restricted by law. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.4.a** Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. | **Describe how** it was observed that a visitor log is in use to record physical access to: | | | | | | |
| * The facility |  | | | | | |
| * Computer rooms and data centers where cardholder data is stored or transmitted. |  | | | | | |
| **9.4.4.b** Verify that the log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. | **Provide the name of the assessor** who attests that the visitor log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. |  | | | | | |
| **9.4.4.c** Verify that the log is retained for at least three months. | **Describe how** visitor logs were observed to be retained for at least three months. |  | | | | | |
| **9.5** Physically secure all media. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.5** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). | **Identify the documented procedures for protecting cardholder data** reviewed to verify controls for physically securing all media are defined. |  | | | | | |
| **9.5.1** Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.5.1** Verify that the storage location security is reviewed at least annually to confirm that backup media storage is secure. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  | | | | | |
| **9.6** Maintain strict control over the internal or external distribution of any kind of media, including the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  | | | | | |
| **9.6.1** Classify media so the sensitivity of the data can be determined. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6.1** Verify that all media is classified so the sensitivity of the data can be determined. | **Describe how** media was observed to be classified so the sensitivity of the data can be determined. |  | | | | | |
| **9.6.2** Send the media by secured courier or other delivery method that can be accurately tracked. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6.2.a** Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. | **Identify** **the responsible personnel** interviewed who confirm that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. |  | | | | | |
| **Identify the records** examined for this testing procedure. |  | | | | | |
| **Describe how** the offsite tracking records verified that all media is logged and sent via secured courier or other delivery method that can be tracked. |  | | | | | |
| **9.6.2.b** Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented. | **Identify the sample** of recent offsite tracking logs for all media selected. |  | | | | | |
| *For each item in the sample,* **describe how** tracking details were observed to be documented. |  | | | | | |
| **9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.6.3** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | **Identify** **the** **responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  | | | | | |
| *For each item in the sample in 9.6.2.b,* **describe how** proper management authorization was observed to be obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  | | | | | |
| **9.7** Maintain strict control over the storage and accessibility of media. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.7** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. | **Identify the documented policy** **for controlling storage and maintenance of all media** that was reviewed to verify that the policy defines required periodic media inventories. |  | | | | | |
| **9.7.1** Properly maintain inventory logs of all media and conduct media inventories at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.7.1** Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually. | **Identify the media inventory logs** reviewed. |  | | | | | |
| **Describe how** the media inventory logs verified that: | | | | | | |
| * Media inventory logs of all media were observed to be maintained. |  | | | | | |
| * Media inventories are performed at least annually. |  | | | | | |
| **9.8** Destroy media when it is no longer needed for business or legal reasons as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.8** Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). |  | | | | | |
| **9.8.1** Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.8.1.a** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | **Identify** **the responsible personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  | | | | | |
| **Provide the name of the assessor** who attests that the procedures state that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. |  | | | | | |
| **9.8.1.b** Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured. | **Describe how** the storage containers used for materials to be destroyed were verified to be secured. |  | | | | | |
| **9.8.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.8.2** Verify that cardholder data on electronic media is rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. |  | | | | | |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify the industry-accepted standards** used. |  | | | | | |
| **9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.  **Note:** These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9** Examine documented policies and procedures to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. | **Identify the documented policies and procedures** examined to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. |  | | | | | |
| **9.9.1** Maintain an up-to-date list of devices. The list should include the following:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9.1.a** Examine the list of devices to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | **Identify the documented up-to-date list of devices** examined to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. |  | | | | | |
| **9.9.1.b** Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date. | **Identify the sample** of devices from the list selected for this testing procedure. |  | | | | | |
| *For all items in the sample,* **describe how** the devices and device locations were observed to verify that the list is accurate and up-to-date. |  | | | | | |
| **9.9.1.c** Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc. | **Identify the responsible personnel** interviewed who confirm the list of devices is updated when devices are added, relocated, decommissioned, etc. |  | | | | | |
| **9.9.2** Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).  **Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9.2.a** Examine documented procedures to verify processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. | **Identify** **the documented procedures** examined to verify that processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. |  | | | | | |
| **9.9.2.b** Interview responsible personnel and observe inspection processes to verify:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. | **Identify** the **responsible personnel** interviewed who confirm that:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. |  | | | | | |
| **Describe how** inspection processes were observed to verify that: | | | | | | |
| * All devices are periodically inspected for evidence of tampering. |  | | | | | |
| * All devices are periodically inspected for evidence of substitution. |  | | | | | |
| **9.9.3** Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:   * Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Do not install, replace, or return devices without verification. * Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.9.3.a** Review training materials for personnel at point-of-sale locations to verify it includes training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | **Identify** **the training materials for personnel at point-of-sale locations** that were reviewed to verify the materials include training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting all suspicious behavior to appropriate personnel (for example, a manager or security officer). * Reporting tampering or substitution of devices. |  | | | | | |
| **9.9.3.b** Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | **Identify** **the sample** of personnel at point-of-sale locations interviewed. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify interviewees have received training and are aware of the procedures for the following: | | | | | | |
| * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. |  | | | | | |
| * Not to install, replace, or return devices without verification. |  | | | | | |
| * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). |  | | | | | |
| * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). |  | | | | | |
| **9.10** Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.10** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting physical access to cardholder data are documented. |  | | | | | |
| Identify the **responsible personnel interviewed** who confirm that the above documented security policies and operational procedures for restricting physical access to cardholder data are:   * In use, and * Known to all affected parties. |  | | | | | |

### Regularly Monitor and Test Networks

#### Requirement 10: Track and monitor all access to network resources and cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **10.1** Implement audit trails to link all access to system components to each individual user. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.1** Verify, through observation and interviewing the system administrator, that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. | **Identify the system administrator(s)** interviewed who confirm that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. |  | | | | | |
| **Describe how** audit trails were observed to verify the following: | | | | | | |
| * Audit trails are enabled and active for system components. |  | | | | | |
| * Access to system components is linked to individual users. |  | | | | | |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following: | **Identify the responsible personnel** interviewed who confirm the following from 10.2.1-10.2.7 are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  | | | | | |
| **Identify the sample of audit logs** selected for 10.2.1-10.2.7. |  | | | | | |
| **10.2.1** All individual user accesses to cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1** Verify all individual access to cardholder data is logged. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all individual access to cardholder data is logged. |  | | | | | |
| **10.2.2** All actions taken by any individual with root or administrative privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.2** Verify all actions taken by any individual with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all actions taken by any individual with root or administrative privileges are logged. |  | | | | | |
| **10.2.3** Access to all audit trails. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.3** Verify access to all audit trails is logged. | *For all items in the sample at 10.2*, **describe how** audit logs and audit log settings verified that access to all audit trails is logged. |  | | | | | |
| **10.2.4** Invalid logical access attempts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.4** Verify invalid logical access attempts are logged. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that invalid logical access attempts are logged. |  | | | | | |
| **10.2.5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.5.a** Verify use of identification and authentication mechanisms is logged. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that use of identification and authentication mechanisms is logged. |  | | | | | |
| **10.2.5.b** Verify all elevation of privileges is logged. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all elevation of privileges is logged. |  | | | | | |
| **10.2.5.c** Verify all changes, additions, or deletions to any account with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all changes, additions, or deletions to any account with root or administrative privileges are logged. |  | | | | | |
| **10.2.6** Initialization, stopping, or pausing of the audit logs. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.6** Verify the following are logged:   * Initialization of audit logs. * Stopping or pausing of audit logs. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that initialization of audit logs is logged. |  | | | | | |
| *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that stopping and pausing of audit logs is logged. |  | | | | | |
| **10.2.7** Creation and deletion of system-level objects. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.7** Verify creation and deletion of system level objects are logged. | *For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that creation and deletion of system level objects are logged. |  | | | | | |
| **10.3** Record at least the following audit trail entries for all system components for each event: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following: | **Identify the responsible personnel** interviewed who confirm that for each auditable event from 10.2.1-10.2.7, the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | |
| **Identify the sample of audit logs** from 10.2.1-10.2.7 observed to verify the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | |
| **10.3.1** User identification | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.1** Verify user identification is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that user identification is included in log entries. |  | | | | | |
| **10.3.2** Type of event | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.2** Verify type of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that type of event is included in log entries. |  | | | | | |
| **10.3.3** Date and time | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.3** Verify date-and-time stamp is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that date and time stamp is included in log entries. |  | | | | | |
| **10.3.4** Success or failure indication | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.4** Verify success or failure indication is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that success or failure indication is included in log entries. |  | | | | | |
| **10.3.5** Origination of event | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.5** Verify origination of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that origination of event is included in log entries. |  | | | | | |
| **10.3.6** Identity or name of affected data, system component, or resource | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs verified that the identity or name of affected data, system component, or resource is included in log entries. |  | | | | | |
| **10.4** Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.  ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. | **Identify** the time-synchronization technologies in use. (If NTP, include version) |  | | | | | |
| **Identify** **the documented time-synchronization configuration standards** examined to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. |  | | | | | |
| **Describe how** processes were examined to verify that time synchronization technologies are: | | | | | | |
| * Implemented. |  | | | | | |
| * Kept current, per the documented process. |  | | | | | |
| **10.4.1** Critical systems have the correct and consistent time. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. * Systems receive time information only from designated central time server(s). | **Describe how** theprocess for acquiring, distributing, and storing the correct time within the organization was examined to verify the following: | | | | | | |
| * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. |  | | | | | |
| * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. |  | | | | | |
| * Systems receive time information only from designated central time server(s). |  | | | | | |
| **10.4.1.b** Observe the time-related system-parameter settings for a sample of system components to verify:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. * Systems receive time only from designated central time server(s). | **Identify the sample** of system components selected for 10.4.1.b-10.4.2.b |  | | | | | |
| *For all items in the sample,* **describe how** the time-related system-parameter settings verified: | | | | | | |
| * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. |  | | | | | |
| * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. |  | | | | | |
| * Systems receive time only from designated central time server(s). |  | | | | | |
| **10.4.2** Time data is protected. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data. | *For all items in the sample from 10.4.1,* **describe how** configuration settings verified that access to time data is restricted to only personnel with a business need to access time data. |  | | | | | |
| **10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. | *For all items in the sample from 10.4.1,* **describe how** configuration settings and time synchronization settings verified that any changes to time settings on critical systems are logged. |  | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** the examined logs verified that any changes to time settings on critical systems are logged. |  | | | | | |
| **Describe how** time synchronization processes were examined to verify changes to time settings on critical systems are: | | | | | | |
| * Logged |  | | | | | |
| * Monitored |  | | | | | |
| * Reviewed |  | | | | | |
| **10.4.3** Time settings are received from industry-accepted time sources. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers). | **Identify the sample** of time servers selected for this testing procedure. |  | | | | | |
| *For all items in the sample,* **describe how** configuration settings verified either of the following: | | | | | | |
| * That the time servers receive time updates from specific, industry-accepted external sources. OR |  | | | | | |
| * That time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines. |  | | | | | |
| **10.5** Secure audit trails so they cannot be altered. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows: | **Identify the system administrators** interviewed who confirm that audit trails are secured so that they cannot be altered as follows (from 10.5.1-10.5.5):   * Only individuals who have a job-related need can view audit trail files. * Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. * Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, including:   That current audit trail files are promptly backed up to the centralized log server or media  The frequency that audit trail files are backed up  That the centralized log server or media is difficult to alter   * Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. * Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. |  | | | | | |
| **Identify the sample** of system components selected for 10.5.1-10.5.5. |  | | | | | |
| **10.5.1** Limit viewing of audit trails to those with a job-related need. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.1** Only individuals who have a job-related need can view audit trail files. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that only individuals who have a job-related need can view audit trail files. |  | | | | | |
| **10.5.2** Protect audit trail files from unauthorized modifications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. |  | | | | | |
| **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.3** Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. |  | | | | | |
| **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.4** Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that logs for external-facing technologies are written onto a secure, centralized, internal log server or media. |  | | | | | |
| **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5.5** Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs. | *For each item in the sample at 10.5,* **describe how** the following verified the use of file-integrity monitoring or change-detection software on logs: | | | | | | |
| * System settings |  | | | | | |
| * Monitored files |  | | | | | |
| * Results from monitoring activities |  | | | | | |
| **Identify** the file-integrity monitoring (FIM) or change-detection software verified to be in use. |  | | | | | |
| **10.6** Review logs and security events for all system components to identify anomalies or suspicious activity.  **Note:** Log harvesting, parsing, and alerting tools may be used to meet this Requirement. | | | | | | | |
| **10.6** Perform the following: | | | | | | | |
| **10.6.1** Review the following at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.6.1.a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | **Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | |
| **Describe** the manual or log tools used for daily review of logs. |  | | | | | |
| **10.6.1.b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | **Identify the responsible personnel** interviewed who confirm that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | | | | | | |
| * All security events. |  | | | | | |
| * Logs of all system components that store, process, or transmit CHD and/or SAD. |  | | | | | |
| * Logs of all critical system components. |  | | | | | |
| * Logs of all servers and system components that perform security functions. |  | | | | | |
| **10.6.2** Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. | **Identify** **the documented security policies and procedures** examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. |  | | | | | |
| **Describe the manual or log tools** defined for periodic review of logs of all other system components. |  | | | | | |
| **10.6.2.b** Examine the organization’s risk assessment documentation and interview personnel to verify that reviews are performed in accordance with organization’s policies and risk management strategy. | **Identify** **the organization’s risk assessment documentation** examined to verify that reviews are performed in accordance with the organization’s policies and risk management strategy. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that reviews are performed in accordance with organization’s policies and risk management strategy. |  | | | | | |
| **10.6.3** Follow up exceptions and anomalies identified during the review process. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | **Identify** **the documented security policies and procedures** examined to verify that procedures define following up on exceptions and anomalies identified during the review process. |  | | | | | |
| **10.6.3.b** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. | **Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed. |  | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that follow-up to exceptions and anomalies is performed. |  | | | | | |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.7.a** Examine security policies and procedures to verify that they define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. | **Identify** **the documented security policies and procedures** examined to verify that procedures define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. |  | | | | | |
| **10.7.b** Interview personnel and examine audit logs to verify that audit logs are retained for at least one year. | **Identify** **the responsible personnel** interviewed who confirm that audit logs are retained for at least one year. |  | | | | | |
| **Describe how** the audit logs verified that audit logs are retained for at least one year. |  | | | | | |
| **10.7.c** Interview personnel and observe processes to verify that at least the last three months’ logs are immediately available for analysis. | **Identify** **the responsible personnel** interviewed who confirm that at least the last three months’ logs are immediately available for analysis. |  | | | | | |
| **Describe how** processes were observed to verify that at least the last three months’ logs are immediately available for analysis. |  | | | | | |
| **10.8 *Additional requirement for service providers only*:** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:   * Firewalls * IDS/IPS * FIM * Anti-virus * Physical access controls * Logical access controls * Audit logging mechanisms * Segmentation controls (if used) | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.8.a** Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:   * Firewalls * IDS/IPS * FIM * Anti-virus * Physical access controls * Logical access controls * Audit logging mechanisms * Segmentation controls (if used) | **Identify the documented policies and procedures** examined to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:   * Firewalls * IDS/IPS * FIM * Anti-virus * Physical access controls * Logical access controls * Audit logging mechanisms * Segmentation controls (if used) |  | | | | | |
| **10.8.b** Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. | **Identify the responsible personnel** interviewed who confirm that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. |  | | | | | |
| **Describe how** examination of the detection and alerting processes verified that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. |  | | | | | |
| **10.8.1 *Additional requirement for service providers only*:** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.8.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls | **Identify the documented policies and procedures** examined to verify that processes are defined and implemented to respond to a security control failure, and include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that processes are defined and implemented to respond to a security control failure, and include:   * Restoring security functions * Identifying and documenting the duration (date and time start to end) of the security failure * Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause * Identifying and addressing any security issues that arose during the failure * Performing a risk assessment to determine whether further actions are required as a result of the security failure * Implementing controls to prevent cause of failure from reoccurring * Resuming monitoring of security controls |  | | | | | |
| **10.8.1.b** Examine records to verify that security control failures are documented to include:   * Identification of cause(s) of the failure, including root cause * Duration (date and time start and end) of the security failure * Details of the remediation required to address the root cause | **Identify the sample of records** examined to verify that security control failures are documented to include:   * Identification of cause(s) of the failure, including root cause * Duration (date and time start and end) of the security failure * Details of the remediation required to address the root cause |  | | | | | |
| *For each sampled record,* **describe how** the documented security control failures include:   * Identification of cause(s) of the failure, including root cause * Duration (date and time start and end) of the security failure * Details of the remediation required to address the root cause |  | | | | | |
| **10.9** Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.9** Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for monitoring all access to network resources and cardholder data are:   * In use * Known to all affected parties |  | | | | | |

#### Requirement 11: Regularly test security systems and processes

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.  **Note:** Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.  Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.a** Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis. | **Identify** **the documented policies and procedures** examined to verify processes are defined for detection and identification of authorized and unauthorized wireless access points on a quarterly basis. |  | | | | | |
| **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:   * WLAN cards inserted into system components. * Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). * Wireless devices attached to a network port or network device. | **Provide the name of the assessor** who attests that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:   * WLAN cards inserted into system components. * Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). * Wireless devices attached to a network port or network device. |  | | | | | |
| **11.1.c If wireless scanning is utilized,** examine output from recent wireless scans to verify that:   * Authorized and unauthorized wireless access points are identified, and * The scan is performed at least quarterly for all system components and facilities. | **Indicate whether** wireless scanning is utilized. **(yes/no)**  *If ‘no,’ mark the remainder of 11.1.c as ‘not applicable.’* |  | | | | | |
| *If ‘yes,’* **Identify/describe** the output from recent wireless scans examined to verify that:   * Authorized wireless access points are identified. * Unauthorized wireless access points are identified. * The scan is performed at least quarterly. * The scan covers all system components. * The scan covers all facilities. |  | | | | | |
| **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel. | **Indicate** **whether** automated monitoring is utilized. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 11.1.d as “Not Applicable.”*  *If “yes,” complete the following:* | | | | | | |
| **Identify and describe** any automated monitoring technologies in use. |  | | | | | |
| *For each monitoring technology in use,* **describe how** the technology generates alerts to personnel. |  | | | | | |
| **11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.1** Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. | **Identify** **the documented inventory records** of authorized wireless access points examined to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. |  | | | | | |
| **11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.2.a** Examine the organization’s incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected. | **Identify the Incident Response Plan document** examined that defines and requires response in the event that an unauthorized wireless access point is detected. |  | | | | | |
| **11.1.2.b** Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found. | **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that action is taken when unauthorized wireless access points are found. |  | | | | | |
| *And/or:* | | | | | | |
| **Identify the recent wireless scans** inspected for this testing procedure. |  | | | | | |
| **Describe how** the recent wireless scans and related responses verified that action is taken when unauthorized wireless access points are found. |  | | | | | |
| **11.2** Run internal and external network vulnerability scans at least quarterly andafter any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).  **Note:** Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.  For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2** Examine scan reports and supporting documentation toverify that internal and external vulnerability scans are performed as follows: | | | | | | | |
| **11.2.1** Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high-risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. | **Identify** **the internal vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly internal scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.1.b** Review the scan reports and verify that all “high-risk” vulnerabilities are addressed and the scan process includes rescans to verify that the “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | **Identify the documented process for quarterly internal scanning** to verify the process defines performing rescans as part of the quarterly internal scan process. |  | | | | | |
| *For each of the four internal quarterly scans indicated at 11.2.1.a*, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes,”* **describe how** rescans were verified to be performed until all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. |  | | | | | |
| **11.2.1.c** Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Identify the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| **Indicate** **whether** a qualified internal resource performs the scan. **(yes/no)**  *If “no,” mark the remainder of 11.2.1.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify: | | | | | | |
| * The scan was performed by a qualified internal resource |  | | | | | |
| * Organizational independence of the tester exists. |  | | | | | |
| **11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.  **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).  Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period. | **Identify** **the external network vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly external vulnerability scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.2.b** Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures). | **Provide the name of the assessor** who attests that the results of each quarterly scan were reviewed and verified that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| *For each of the four external quarterly scans indicated at 11.2.2.a*, **indicate whether** a rescan was necessary. **(yes/no)** |  | | | | | |
| *If “yes,”* **describe how** the results of the rescan verified that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| **11.2.2.c** Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV). | **Provide the name of the assessor** who attests that the external scan reports were reviewed and verified to have been completed by a PCI SSC-Approved Scanning Vendor (ASV). |  | | | | | |
| **11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.3.a** Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned. | **Identify the change control documentation and scan reports** reviewed for this testing procedure. |  | | | | | |
| **Describe how** the change control documentation and scan reports verified that all system components subject to significant change were scanned after the change. |  | | | | | |
| **11.2.3.b** Review scan reports and verify that the scan process includes rescans until:   * For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. * For internal scans, all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | For all scans reviewed in 11.2.3.a, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes”* – for external scans, **describe how** rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist. |  | | | | | |
| *If “yes”* – for internal scans, **describe how** rescans were performed until either passing results were obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved. |  | | | | | |
| **11.2.3.c** Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Indicate whether** an internal resource performed the scans. **(yes/no)**  *If “no,” mark the remainder of 11.2.3.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the scans demonstrated they are qualified to perform the scans. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3** Implement a methodology for penetration testing that includes at least the following:   * Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside of the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3** Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented and includes at least the following:   * Is based on industry-accepted penetration testing approaches. * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results. | **Identify the documented penetration-testing methodology** examined to verify a methodology is implemented that includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm the penetration–testing methodology implemented includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
| **11.3.1** Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.1.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented external penetration test results** reviewed to verify that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work verified that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Identify whether** any significant external infrastructure or application upgrade or modification occurred during the past 12 months. |  | | | | | |
| **Identify** **the documented penetration test results reviewed** to verify that external penetration tests are performed after significant external infrastructure or application upgrade. |  | | | | | |
| **11.3.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Indicate whether** an internal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.1.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.2** Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented internal penetration test results** reviewed to verify that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work verified that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Indicate whether** any significant internal infrastructure or application upgrade or modification occurred during the past 12 months. **(yes/no)** |  | | | | | |
| **Identify** **the documented internal penetration test results** reviewed to verify that internal penetration tests are performed after significant internal infrastructure or application upgrade. |  | | | | | |
| **11.3.2.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Indicate whether** an internal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.2.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.3** Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.3** Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. | **Identify the documented penetration testing results** examined to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. |  | | | | | |
| **11.3.4** If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.4.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Indicate** **whether** segmentation is used to isolate the CDE from other networks. **(yes/no)**  *If “no,” mark the remainder of 11.3.4.a, 11.3.4.b and 11.3.4.c as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **identify the defined penetration-testing methodology** examined to verify procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **Describe how** the segmentation controls verified that segmentation methods: | | | | | | |
| * Are operational and effective. |  | | | | | |
| * Isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.3.4.b** Examine the results from the most recent penetration test to verify that:   * Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Identify the documented results from the most recent penetration test** examined to verify that:   * Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.3.4.c** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.4.1 *Additional requirement for service providers only*:** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.4.1.a** Examine the results from the most recent penetration test to verify that:   * Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | **Identify the documented results from the most recent penetration test** examined to verify that:   * Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. * The penetration testing covers all segmentation controls/methods in use. * The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **11.3.4.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.4** Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.  Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. | **Identify the network diagrams** examined to verify that techniques are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. |  | | | | | |
| **Describe how** system configurations verified that techniques are in place to monitor all traffic: | | | | | | |
| * At the perimeter of the cardholder data environment. |  | | | | | |
| * At critical points in the cardholder data environment. |  | | | | | |
| **11.4.b** Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. | **Describe how** system configurations for intrusion-detection and/or intrusion-prevention techniques verified that they are configured to alert personnel of suspected compromises. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the generated alerts are received as intended. |  | | | | | |
| **11.4.c** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | **Identify** **the vendor document(s)** examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques. |  | | | | | |
| **Describe how** IDS/IPS configurations and vendor documentation verified that intrusion-detection, and/or intrusion-prevention techniques are: | | | | | | |
| * Configured per vendor instructions to ensure optimal protection. |  | | | | | |
| * Maintained per vendor instructions to ensure optimal protection. |  | | | | | |
| * Updated per vendor instructions to ensure optimal protection. |  | | | | | |
| **11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.  **Note:** For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.a** Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities.  *Examples of files that should be monitored:*   * *System executables* * *Application executables* * *Configuration and parameter files* * *Centrally stored, historical or archived, log and audit files* * *Additional critical files determined by entity (i.e., through risk assessment or other means)* | **Describe** the change-detection mechanism deployed. |  | | | | | |
| **Identify the results** from monitored files reviewed to verify the use of a change-detection mechanism. |  | | | | | |
| **Describe how** the following verified the use of a change-detection mechanism: | | | | | | |
| * System settings |  | | | | | |
| * Monitored files |  | | | | | |
| **11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly. | **Describe how** system settings verified that the change-detection mechanism is configured to: | | | | | | |
| * Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files. |  | | | | | |
| * Perform critical file comparisons at least weekly. |  | | | | | |
| **11.5.1** Implement a process to respond to any alerts generated by the change-detection solution. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.1** Interview personnel to verify that all alerts are investigated and resolved. | **Identify the responsible personnel** interviewed who confirm that all alerts are investigated and resolved |  | | | | | |
| **11.6** Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.6** Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for security monitoring and testing are documented. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for security monitoring and testing are:   * In use * Known to all affected parties |  | | | | | |

### Maintain an Information Security Policy

#### Requirement 12: Maintain a policy that addresses information security for all personnel

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **12.1** Establish, publish, maintain, and disseminate a security policy. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  | | | | | |
| **Describe how** the information security policy was verified to be published and disseminated to: | | | | | | |
| * All relevant personnel. |  | | | | | |
| * All relevant vendors and business partners. |  | | | | | |
| **12.1.1** Review the security policy at least annually and update the policy when business objectives or the risk environment change. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1.1** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | **Describe how** the information security policy was verified to be: | | | | | | |
| * Reviewed at least annually. |  | | | | | |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  | | | | | |
| **12.2** Implement a risk assessment process, that:   * Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), * Identifies critical assets, threats, and vulnerabilities, and * Results in a formal, documented analysis of risk.   *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.2.a** Verify that an annual risk-assessment process is documented that:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. | **Provide the name of the assessor** who attests that the documented annual risk-assessment process:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. |  | | | | | |
| **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | **Identify the risk assessment result documentation** reviewed to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. |  | | | | | |
| **12.3** Develop usage policies for critical technologies and define proper use of these technologies.  **Note:** Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.  Ensure these usage policies require the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed: | **Identify** critical technologies in use. |  | | | | | |
| **Identify the usage policies for all identified critical technologies** reviewed to verify the following policies (12.3.1-12.3.10) are defined:   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **Identify the responsible** **personnel** interviewed who confirm usage policies for all identified critical technologies are implemented and followed (for 12.3.1–12.3.10):   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.1** Explicit approval by authorized parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.1** Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to include processes for explicit approval from authorized parties to use the technologies. |  | | | | | |
| **12.3.2** Authentication for use of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.2** Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token). | **Provide the name of the assessor** who attests that the usage policies were verified to include processes for all technology use to be authenticated with user ID and password or other authentication item. |  | | | | | |
| **12.3.3** A list of all such devices and personnel with access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.3** Verify that the usage policies define:   * A list of all critical devices, and * A list of personnel authorized to use the devices. | **Provide the name of the assessor** who attests that the usage policies were verified to define:   * A list of all critical devices, and * A list of personnel authorized to use the devices. |  | | | | | |
| **12.3.4** A method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.4** Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | **Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine:   * Owner * Contact Information * Purpose |  | | | | | |
| **12.3.5** Acceptable uses of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.5** Verify that the usage policies define acceptable uses for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  | | | | | |
| **12.3.6** Acceptable network locations for the technologies. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.6** Verify that the usage policies define acceptable network locations for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable network locations for the technology. |  | | | | | |
| **12.3.7** List of company-approved products. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.7** Verify that the usage policies include a list of company-approved products. | **Provide the name of the assessor** who attests that the usage policies were verified to include a list of company-approved products. |  | | | | | |
| **12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.8.a** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | **Provide the name of the assessor** who attests that the usage policies were verified to require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. |  | | | | | |
| **12.3.8.b** Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity. | **Identify** any remote access technologies in use |  | | | | | |
| **Describe how** configurations for remote access technologies verified that remote access sessions will be automatically disconnected after a specific period of inactivity. |  | | | | | |
| **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | **Provide the name of the assessor** who attests that the usage policies were verified to require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. |  | | | | | |
| **12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to prohibit copying, moving or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements. | **Provide the name of the assessor** who attests that the usage policies were verified to require, for personnel with proper authorization, the protection of cardholder data in accordance with PCI DSS Requirements. |  | | | | | |
| **12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.4.a** Verify that information security policy and procedures clearly define information security responsibilities for all personnel. | **Identify** **the information security policy and procedures** reviewed to verify that they clearly define information security responsibilities for all personnel. |  | | | | | |
| **12.4.b** Interview a sample of responsible personnel to verify they understand the security policies. | **Identify the responsible personnel** interviewed for this testing procedure who confirm they understand the security policy. |  | | | | | |
| **12.4.1 *Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:   * Overall accountability for maintaining PCI DSS compliance * Defining a charter for a PCI DSS compliance program and communication to executive management | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.4.1.a** Examine documentation to verify executive management has assigned overall accountability for maintaining the entity’s PCI DSS compliance | **Identify the documentation** examined to verify thatexecutive management has assigned overall accountability for maintaining the entity’s PCI DSS compliance. |  | | | | | |
| **12.4.1.b** Examine the company’s PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management. | **Identify the company’s PCI DSS charter** examined to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management. |  | | | | | |
| **12.5** Assign to an individual or team the following information security management responsibilities: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5** Examine information security policies and procedures to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: | **Identify** **the information security policies and procedures** reviewed to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: |  | | | | | |
| **12.5.1** Establish, document, and distribute security policies and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.1** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security policies and procedures. * Documenting security policies and procedures. * Distributing security policies and procedures. |  | | | | | |
| **12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring and analyzing security alerts. * Distributing information to appropriate information security and business unit management personnel. |  | | | | | |
| **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.3** Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security incident response and escalation procedures. * Documenting security incident response and escalation procedures. * Distributing security incident response and escalation procedures. |  | | | | | |
| **12.5.4** Administer user accounts, including additions, deletions, and modifications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.4** Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for administering user account and authentication management. |  | | | | | |
| **12.5.5** Monitor and control all access to data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring all access to data * Controlling all access to data |  | | | | | |
| **12.6** Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.a** Review the security awareness program to verify it provides awareness to all personnel about the cardholder data security policy and procedures. | **Provide the name of the assessor** who attests that the security awareness program was verified to provide awareness to all personnel about the cardholder data security policy and procedures. |  | | | | | |
| **12.6.b** Examine security awareness program procedures and documentation and perform the following: | **Identify the documented security awareness program procedures and additional documentation** examined to verify that:   * The security awareness program provides multiple methods of communicating awareness and educating personnel. * Personnel attend security awareness training:   Upon hire, and  At least annually   * Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. |  | | | | | |
| **12.6.1** Educate personnel upon hire and at least annually.  ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel. |  | | | | | |
| **12.6.1.b** Verify that personnel attend security awareness training upon hire and at least annually. | **Describe how** it was observed that all personnel attend security awareness training: | | | | | | |
| * Upon hire |  | | | | | |
| * At least annually |  | | | | | |
| **12.6.1.c** Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security. | **Identify the sample** of personnel interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify they have completed awareness training and are aware of the importance of cardholder data security. |  | | | | | |
| **12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. | **Describe how** it was observed that, per the security awareness program, all personnel: | | | | | | |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  | | | | | |
| * Provide an acknowledgement at least annually. |  | | | | | |
| **12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)  **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. | **Identify the Human Resources personnel** interviewed who confirm background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  | | | | | |
| **Describe how** it was observed that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  | | | | | |
| **12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8**Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows: | **Identify the documented policies and procedures** reviewed to verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, per 12.8.1–12.8.5: |  | | | | | |
| **12.8.1** Maintain a list of service providers including a description of the service provided. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.1** Verify that a list of service providers is maintained and includes a list of the services provided. | **Describe how** the documented list of service providers was observed to be maintained (kept up-to-date) and includes a list of the services provided. |  | | | | | |
| **12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE.  ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.2** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | **Describe how** written agreements for each service provider were observed to include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer. |  | | | | | |
| **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Identify the policies and procedures** reviewed to verify that processes included proper due diligence prior to engaging any service provider. |  | | | | | |
| **Describe how** it was observed that the above policies and procedures are implemented. |  | | | | | |
| **12.8.4** Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.4** Verify that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. | **Describe how** it was observed that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. |  | | | | | |
| **12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.5** Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | **Describe how** it was observed that the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  | | | | | |
| **12.9 *Additional requirement for service providers only*:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.  **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.9 *Additional testing procedure for service provider assessments only****:*Review service provider’s policies and procedures and observe templates used for written agreement to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | **Indicate whether** the assessed entity is a service provider. **(yes/no)**  *If “no,” mark the remainder of 12.9 as “Not Applicable.”*  *If “yes”:* |  | | | | | |
| **Identify the service provider’s policies and procedures** reviewed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **Describe how** the templates used for written agreement verified that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following: | **Identify** **the documented incident response plan and related procedures** examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows from 12.10.1–12.10.6:   * Create the incident response plan to be implemented in the event of system breach. * Test the plan at least annually. * Designate specific personnel to be available on a 24/7 basis to respond to alerts:   24/7 incident monitoring  24/7 incident response   * Provide appropriate training to staff with security breach response responsibilities. * Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. * Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  | | | | | |
| **12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:   * Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage and responses of all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.1.a** Verify that the incident response plan includes:   * Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures * Data back-up processes * Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). * Coverage and responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  | | | | | |
| **12.10.1.b** Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed. | **Identify the responsible** **personnel** interviewed who confirm that the documented incident response plan and procedures are followed. |  | | | | | |
| **Identify the sample** of previously reported incidents or alerts selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** the documented incident response plan and procedures were observed to be followed. |  | | | | | |
| **12.10.2** Review and test the plan at least annually, including all elements listed in Requirement 12.10.1. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.2** Interview personnel and review documentation from testing to verify that the plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1. | **Identify the responsible personnel** interviewed who confirm that the incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1. |  | | | | | |
| **Identify documentation** reviewed from testing to verify thatthe incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1. |  | | | | | |
| **12.10.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes. | **Identify** **the document** requiring 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **Describe how** it was observed that designated personnel are available for 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **12.10.4** Provide appropriate training to staff with security breach response responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.4** Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained. | **Identify the responsible personnel** interviewed who confirm that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Identify the documented policy** reviewed to verify that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Describe how** it was observed that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **12.10.5** Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan. | **Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **Describe how** processes were reviewed to verify that ***responding to*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **12.10.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.6** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | | | | | | |
| * According to lessons learned. |  | | | | | |
| * To incorporate industry developments. |  | | | | | |
| **12.11 Additional requirement for service providers only:** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:   * Daily log reviews * Firewall rule-set reviews * Applying configuration standards to new systems * Responding to security alerts * Change management processes | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.11.a** Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover:   * Daily log reviews * Firewall rule-set reviews * Applying configuration standards to new systems * Responding to security alerts * Change management processes | **Identify the policies and procedures** examined to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover:   * Daily log reviews * Firewall rule-set reviews * Applying configuration standards to new systems * Responding to security alerts * Change management processes |  | | | | | |
| **12.11.b** Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly | **Identify the document(s) related to reviews** examined to verify that reviews are performed at least quarterly. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that reviews are performed at least quarterly |  | | | | | |
| **12.11.1 *Additional requirement for service providers only*:** Maintain documentation of quarterly review process to include:   * Documenting results of the reviews * Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.11.1.a** Examine documentation from the quarterly reviews to verify they include:   * Documenting results of the reviews. * Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program. | **Identify the document(s) related to quarterly reviews** to verify they include:   * Documenting results of the reviews. * Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program. |  | | | | | |