|  |  |
| --- | --- |
|  | Image Technology Systems VISUAL MATRIX™  PCI-DSS v.3.2 Cloud Computing Guidelines  Release 1.x.x.x |

**Table of Contents**

[1. Preface 8](#_Toc466468927)

[Revision History 8](#_Toc466468928)

[2. Executive Summary 9](#_Toc466468929)

[The 12 Requirements of the PCI DSS: 9](#_Toc466468930)

[3. Considerations for the Implementation of Payment Application in a PCI-Compliant Environment 11](#_Toc466468931)

[Requirement 1: Install and maintain a firewall configuration to protect cardholder data. 11](#_Toc466468932)

[PCI-DSS Requirement 1.1.1 11](#_Toc466468933)

[Procedure 11](#_Toc466468934)

[PCI-DSS Requirement 1.1.4 11](#_Toc466468935)

[Procedure 11](#_Toc466468936)

[PCI-DSS Requirement 1.1.5 12](#_Toc466468937)

[Procedure 12](#_Toc466468938)

[PCI-DSS Requirement 1.1.6 12](#_Toc466468939)

[Procedure 12](#_Toc466468940)

[PCI-DSS Requirement 1.1.7 13](#_Toc466468941)

[Procedure 13](#_Toc466468942)

[PCI-DSS Requirement 1.2.1 13](#_Toc466468943)

[Procedure 13](#_Toc466468944)

[PCI-DSS Requirement 1.3.7 14](#_Toc466468945)

[Procedure 14](#_Toc466468946)

[PCI-DSS Requirement 1.4 14](#_Toc466468947)

[Procedure 15](#_Toc466468948)

[PCI-DSS Requirement 1.5 15](#_Toc466468949)

[Procedure 15](#_Toc466468950)

[Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. 16](#_Toc466468951)

[PCI-DSS Requirement 2.1 16](#_Toc466468952)

[Procedure 16](#_Toc466468953)

[PCI-DSS Requirement 2.1.1 16](#_Toc466468954)

[Procedure 17](#_Toc466468955)

[PCI-DSS Requirement 2.2 17](#_Toc466468956)

[Procedure 18](#_Toc466468957)

[PCI-DSS Requirement 2.2.4 18](#_Toc466468958)

[Procedure 18](#_Toc466468959)

[PCI-DSS Requirement 2.2.5 18](#_Toc466468960)

[Procedure 18](#_Toc466468961)

[PCI-DSS Requirement 2.3 19](#_Toc466468962)

[Procedure 19](#_Toc466468963)

[PCI-DSS Requirement 2.5 19](#_Toc466468964)

[Procedures 20](#_Toc466468965)

[Requirement 3: Protect stored cardholder data 20](#_Toc466468966)

[PCI-DSS Requirement 3.1 20](#_Toc466468967)

[Procedure 20](#_Toc466468968)

[PCI-DSS Requirements 3.2 20](#_Toc466468969)

[Procedure 21](#_Toc466468970)

[PCI-DSS Requirements 3.3 21](#_Toc466468971)

[Procedure 22](#_Toc466468972)

[PCI-DSS Requirements 3.4 22](#_Toc466468973)

[Procedure 22](#_Toc466468974)

[PCI-DSS Requirements 3.5 22](#_Toc466468975)

[Procedure 22](#_Toc466468976)

[PCI-DSS Requirements 3.5.1 22](#_Toc466468977)

[Procedure 22](#_Toc466468978)

[PCI-DSS Requirements 3.5.3 22](#_Toc466468979)

[Procedure 23](#_Toc466468980)

[PCI-DSS Requirements 3.6 23](#_Toc466468981)

[Procedure 23](#_Toc466468982)

[PCI-DSS Requirements 3.6.1 23](#_Toc466468983)

[Procedure 23](#_Toc466468984)

[PCI-DSS Requirements 3.6.2 23](#_Toc466468985)

[Procedure 23](#_Toc466468986)

[PCI-DSS Requirements 3.6.3 23](#_Toc466468987)

[PCI-DSS Requirements 3.6.4 23](#_Toc466468988)

[Procedure 23](#_Toc466468989)

[PCI-DSS Requirements 3.6.5 23](#_Toc466468990)

[Procedure 23](#_Toc466468991)

[PCI-DSS Requirements 3.6.6 23](#_Toc466468992)

[Procedure 24](#_Toc466468993)

[PCI-DSS Requirements 3.6.7 24](#_Toc466468994)

[Procedure 24](#_Toc466468995)

[PCI-DSS Requirements 3.6.8 24](#_Toc466468996)

[Procedure 24](#_Toc466468997)

[PCI-DSS Requirements 3.7 24](#_Toc466468998)

[PCI-DSS Requirements 4.1 24](#_Toc466468999)

[Procedure 24](#_Toc466469000)

[PCI-DSS Requirements 4.1.1 24](#_Toc466469001)

[Procedure 24](#_Toc466469002)

[PCI-DSS Requirements 4.2 24](#_Toc466469003)

[Procedure 24](#_Toc466469004)

[PCI-DSS Requirements 4.3 24](#_Toc466469005)

[Procedure 25](#_Toc466469006)

[PCI-DSS Requirements 5.11 25](#_Toc466469007)

[Procedure 25](#_Toc466469008)

[PCI-DSS Requirements 5.2 25](#_Toc466469009)

[Procedure 25](#_Toc466469010)

[PCI-DSS Requirements 5.4 25](#_Toc466469011)

[Procedure 25](#_Toc466469012)

[PCI-DSS Requirements 6.1 25](#_Toc466469013)

[Procedure 25](#_Toc466469014)

[PCI-DSS Requirements 6.2 25](#_Toc466469015)

[Procedure 25](#_Toc466469016)

[PCI-DSS Requirements 6.3 25](#_Toc466469017)

[Procedure 26](#_Toc466469018)

[PCI-DSS Requirements 6.3.1 26](#_Toc466469019)

[Procedure 26](#_Toc466469020)

[PCI-DSS Requirements 6.3.2 26](#_Toc466469021)

[Procedure 26](#_Toc466469022)

[PCI-DSS Requirements 6.4 26](#_Toc466469023)

[Procedure 26](#_Toc466469024)

[PCI-DSS Requirements 6.4.1 26](#_Toc466469025)

[Procedure 26](#_Toc466469026)

[PCI-DSS Requirements 6.4.5 26](#_Toc466469027)

[Procedure 26](#_Toc466469028)

[PCI-DSS Requirements 6.5 26](#_Toc466469029)

[Procedure 26](#_Toc466469030)

[PCI-DSS Requirements 6.6 27](#_Toc466469031)

[Procedure 27](#_Toc466469032)

[PCI-DSS Requirements 6.7 27](#_Toc466469033)

[Procedure 27](#_Toc466469034)

[PCI-DSS Requirements 7.1 27](#_Toc466469035)

[Procedure 27](#_Toc466469036)

[PCI-DSS Requirements 7.2.1 27](#_Toc466469037)

[Procedure 27](#_Toc466469038)

[PCI-DSS Requirements 7.3 27](#_Toc466469039)

[Procedure 27](#_Toc466469040)

[PCI-DSS Requirements 8.1 27](#_Toc466469041)

[Procedure 27](#_Toc466469042)

[PCI-DSS Requirements 8.2 27](#_Toc466469043)

[Procedure 28](#_Toc466469044)

[PCI-DSS Requirements 8.2.1 28](#_Toc466469045)

[Procedure 28](#_Toc466469046)

[PCI-DSS Requirements 8.2.2 28](#_Toc466469047)

[Procedure 28](#_Toc466469048)

[PCI-DSS Requirements 8.2.3 28](#_Toc466469049)

[Procedure 28](#_Toc466469050)

[PCI-DSS Requirements 8.2.6 28](#_Toc466469051)

[Procedure 28](#_Toc466469052)

[PCI-DSS Requirements 8.4 28](#_Toc466469053)

[Procedure 28](#_Toc466469054)

[PCI-DSS Requirements 8.5 28](#_Toc466469055)

[Procedure 28](#_Toc466469056)

[PCI-DSS Requirements 8.5.1 29](#_Toc466469057)

[Procedure 29](#_Toc466469058)

[PCI-DSS Requirements 8.6 29](#_Toc466469059)

[Procedure 29](#_Toc466469060)

[PCI-DSS Requirement 8.8 29](#_Toc466469061)

[Procedure 29](#_Toc466469062)

[PCI-DSS Requirements 9.2 29](#_Toc466469063)

[Procedure 29](#_Toc466469064)

[PCI-DSS Requirements 9.4.1 29](#_Toc466469065)

[Procedure 29](#_Toc466469066)

[PCI-DSS Requirements 9.5 29](#_Toc466469067)

[Procedure 29](#_Toc466469068)

[PCI-DSS Requirements 9.6 29](#_Toc466469069)

[Procedure 29](#_Toc466469070)

[PCI-DSS Requirements 9.7 30](#_Toc466469071)

[Procedure 30](#_Toc466469072)

[PCI-DSS Requirements 9.8 30](#_Toc466469073)

[Procedure 30](#_Toc466469074)

[PCI-DSS Requirements 9.9 30](#_Toc466469075)

[Procedure 30](#_Toc466469076)

[PCI-DSS Requirements 9.9.1 30](#_Toc466469077)

[Procedure 30](#_Toc466469078)

[PCI-DSS Requirements 9.9.2 30](#_Toc466469079)

[Procedure 30](#_Toc466469080)

[PCI-DSS Requirements 9.10 30](#_Toc466469081)

[Procedure 30](#_Toc466469082)

[PCI-DSS Requirements 9.9.3 30](#_Toc466469083)

[Procedure 31](#_Toc466469084)

[PCI-DSS Requirements 10.4 31](#_Toc466469085)

[Procedure 31](#_Toc466469086)

[PCI-DSS Requirements 10.6.1 31](#_Toc466469087)

[Procedure 31](#_Toc466469088)

[PCI-DSS Requirements 10.6.2 31](#_Toc466469089)

[Procedure 31](#_Toc466469090)

[PCI-DSS Requirements 10.6.3 31](#_Toc466469091)

[Procedure 31](#_Toc466469092)

[PCI-DSS Requirements 10.7 31](#_Toc466469093)

[Procedure 31](#_Toc466469094)

[PCI-DSS Requirements 10.8 31](#_Toc466469095)

[Procedure 31](#_Toc466469096)

[PCI-DSS Requirements 10.8.1 32](#_Toc466469097)

[Procedure 32](#_Toc466469098)

[PCI-DSS Requirements 10.9 32](#_Toc466469099)

[Procedure 32](#_Toc466469100)

[PCI-DSS Requirements 11.1 32](#_Toc466469101)

[Procedure 32](#_Toc466469102)

[PCI-DSS Requirements 11.1.2 32](#_Toc466469103)

[Procedure 32](#_Toc466469104)

[PCI-DSS Requirements 11.3 32](#_Toc466469105)

[Procedure 32](#_Toc466469106)

[PCI-DSS Requirements 11.4 32](#_Toc466469107)

[Procedure 32](#_Toc466469108)

[PCI-DSS Requirements 11.6 32](#_Toc466469109)

[Procedure 33](#_Toc466469110)

[PCI-DSS Requirements 12.1 33](#_Toc466469111)

[Procedure 33](#_Toc466469112)

[PCI-DSS Requirements 12.2 33](#_Toc466469113)

[Procedure 33](#_Toc466469114)

[PCI-DSS Requirements 12.3 33](#_Toc466469115)

[Procedure 33](#_Toc466469116)

[PCI-DSS Requirements 12.4.1 33](#_Toc466469117)

[Procedure 33](#_Toc466469118)

[PCI-DSS Requirements 12.5 33](#_Toc466469119)

[Procedure 33](#_Toc466469120)

[PCI-DSS Requirements 12.6 33](#_Toc466469121)

[Procedure 33](#_Toc466469122)

[PCI-DSS Requirements 12.8 34](#_Toc466469123)

[Procedure 34](#_Toc466469124)

[PCI-DSS Requirements 12.8.3 34](#_Toc466469125)

[Procedure 34](#_Toc466469126)

[PCI-DSS Requirements 12.9 34](#_Toc466469127)

[Procedure 34](#_Toc466469128)

[PCI-DSS Requirements 12.10 34](#_Toc466469129)

[Procedure 34](#_Toc466469130)

[PCI-DSS Requirements 12.10.2 34](#_Toc466469131)

[Procedure 34](#_Toc466469132)

[PCI-DSS Requirements 12.10.3 34](#_Toc466469133)

[Procedure 34](#_Toc466469134)

[PCI-DSS Requirements 12.10.4 34](#_Toc466469135)

[Procedure 34](#_Toc466469136)

[PCI-DSS Requirements 12.10.6 34](#_Toc466469137)

[Procedure 34](#_Toc466469138)

[PCI-DSS Requirements 12.11 34](#_Toc466469139)

[Procedure 35](#_Toc466469140)

[PCI-DSS Requirements 12.11.1 35](#_Toc466469141)

[Procedure 35](#_Toc466469142)

# 1. Preface

## Revision History

|  |  |
| --- | --- |
| 11/x/2016: Initial Release | Blake Ward |

# 2. Executive Summary

## The 12 Requirements of the PCI DSS:

*Build and Maintain a Secure Network:*

1. Install and maintain a firewall and router configuration to protect cardholder data.
2. Do not use vendor supplied defaults for system passwords and other security paramters.

*Protect Cardholder Data:*

1. Protect stored cardholder data.
2. Encrypt transmission of cardholder data across open, public networks.

*Maintain a Vulnerability Management Program:*

1. Use and regularly update anti-virus software or programs.
2. Develop and maintain secure systems and applications.

*Implement Strong Access Control Measures:*

1. Restrict access to cardholder data by business need to know.
2. Assign a unique ID to each person with computer access.
3. Restrict physical access to cardholder data.

*Regularly Monitor and Test Networks:*

1. Track and monitor all access to network resources and cardholder data.
2. Regularly test security systems and processes.

*Maintain an Information Security Policy:*

1. Maintain a policy that addresses information security for all personnel.

# 3. Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

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

## PCI-DSS Requirement 1.1.1

A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.

Examine documented procedures to verify there is a formal process for testing and approval of all:

* Networks connections
* Changes to firewall and router configurations (1.1.1.a)

### Procedure

Test all n

## PCI-DSS Requirement 1.1.4

Using a firewall on every Internet connection coming into (and out of) the network, and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.

Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. (1.1.4.a)

### Procedure

[Refer to another doc] change

The firewall configuration standards for Visual Matrix™ include firewall at each Internet connection and between any DMZ and the internal network zone. See “Document Title.pdf.”

## PCI-DSS Requirement 1.1.5

This description of roles and assignment of responsibilities ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.

* Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components. (1.1.5.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 1.1.6

Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don’t patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed.

Approvals should be granted by personnel independent of the personnel managing the configuration.

If insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed.

For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (e.g., NIST, ENISA, OWASP, etc.).

* Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each. (1.1.6.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 1.1.7

This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications.

Organizations with a high volume of changes to firewall and router rule sets may wish to consider performing reviews more frequently, to ensure that the rule sets continue to meet the needs of the business.

* Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. (1.1.7.a)
* Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. (1.1.7.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 1.2.1

Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This prevents malicious individuals from accessing the entity’s network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they’ve obtained from within the entity’s network out to an untrusted server).

Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in our out.

* Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment. (1.2.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 1.3.7

Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker “learning” the IP addresses of the internal network, and using that information to access the network.

Methods used to meet the intent of this requirement may vary depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.

* Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized. (1.3.7.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 1.4

Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Inter-based threats. Use of firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization’s systems and data once the device is re-connected to the network.

The specific firewall configuration settings are determined by the organization.

*Note: This requirement applies to employee-owned and company-owned portable computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit. Allowing untrusted systems to connect to and organizations CDE could result in access being granted to attackers and other malicious users.*

Examine policies and configuration 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. (1.4.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 1.5

Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.4

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.

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

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

## PCI-DSS Requirement 2.1

Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack.

Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

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. (2.1.c)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 2.1.1

If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network.

In addition, the key-exchange protocol for older versions 802.11x encryption (Wired Equivalent Privacy, or WEP) has been broken and can render the encryption useless. Firmware for devices should be updated to support more secure protocols.

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. (2.1.1.a)

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 joints are not used. (2.1.1.c)

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.
* Transmissions over wireless networks. (2.1.1.d)

Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable. (2.1.1.e)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 2.2

There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses.

Examples of sources for guidance on configuration standards include, but are not limited to: www.nist.gov, www.sans.org, and www.cisecurity.org, www.iso.org, and product vendors.

System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.

* 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. (2.2.a)
* Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. (2.2.b)
* Examine policies and interview personnel to verify 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.c)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 2.2.4

System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use.

In order for systems to be configured securely, personnel responsible for configuration and/or administering systems must be knowledgeable in the specific security parameters and settings that apply to the system.

* Examine the system configuration standards to verify that common security parameter settings are included. (2.2.4.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 2.2.5

Unnecessary functions can provide additional opportunities for malicious individuals to gain access to a system. By removing unnecessary functionality, organizations can focus on securing the functions that are required and reduce the risk that unknown functions will be exploited.

Including this in server-hardening standards and processes addresses the specific security implications associated with unnecessary functions (for example, by removing/disabling FTP or the web server if the server will not be performing those functions).

* Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components. (2.2.5.c)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 2.3

If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator’s IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data.

Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information.

To be considered “strong cryptography,” industry recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to "strong cryptography” in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms, and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.)

* 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. (2.3.d)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 2.5

Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.

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

### Procedures

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

# Requirement 3: Protect stored cardholder data

## PCI-DSS Requirement 3.1

A formal data retention policy identifies what data needs to be retained, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed.

The only cardholder data that may be stored after authorization is the pimary account number of PAN (rendered unreadable), expiration date, cardholder name, and service code.

Understanding where cardholder data is located is necessary so it can be properly retained or disposed of when no longer needed. In order to define appropriate retention requirements, an entity first needs to understand their own business needs as well as any legal or regulatory obligations that apply to their industry, and/or that apply to the type of data being retained.

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 elgal, 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.

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.2

Sensitive authentication data consists of full track data, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited! This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions.

Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data.

It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements. For non-issuing entities, retaining sensitive authentication data post-authorization is not permitted.

* 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. (3.2.a)
* 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. (3.2.c)
* 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. (3.2.d)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.3

The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data.

The masking approach should always ensure that only the minimum number of digits is displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits. As another example, if a function needs access to the bank identification number (BIN) for routing purposes, unmask only the BIN digits (traditionally the first six digits) during that function.

This requirement relates to protection of PAN displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when stored in files, databases, etc.

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 the 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. (3.3.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.4

PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected.

One-way hash functions based on strong cryptography can be used to render cardholder data unreadable. Hash functions are appropriate when there is no need to retrieve the original number (one-way hashes are irreversible). It is recommended, but not currently a requirement, that an additional, random input value be added to the cardholder data prior to hashing to reduce the feasibility of an attacker comparing the data against (and deriving the PAN from) tables of precomputed hash values.

The intent of truncation is to permanently remove a segment of PAN data so that only a portion (generally not to exceed the first six and last four digits) of the PAN is stored.

An index token is a cryptographic token that replaces the PAN based on a given index for an unpredictable value. A one-time pad is a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted using a matching one-time pad and key.

The intent of strong cryptography (as defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms) is that the encryption be based on an industry-tested and accepted algorithm (not a proprietary or "homegrown" algorithm) with strong cryptographic keys.

By correlating hashed and truncated versions of a given PAN, a malicious individual may easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable.

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 (3.4.A)

## Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.5

Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. Key-encrypting keys, if used, must be at least as strong as the data-encrypting key in order to ensure proper protection of the key that encrypts the data as well as the data encrypted with that key.

The requirement to protect keys from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.

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. (3.5)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.5.1

Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect cardholder data, as well as the devices that generate, use and protect the keys. This allows an entity to keep pace with evolving threats to their architecture, enabling them to plan for updates as the assurance levels provided by different algorithms/key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices, and identify unauthorized additions to their cryptographic architecture.

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 (3.5.1)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.5.3

Cryptographic keys must be stored securely to prevent unauthorized or unnecessary access that could result in the exposure of cardholder data.

It is not intended that the key-encrypting keys be encrypted, however they are to be protected against disclosure and misuse as defined in Requirement 3.5. If key-encrypting keys are used, storing the key-encrypting keys in physically and/or logically separate locations from the data-encrypting keys reduces the risk of unauthorized access to both keys.

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 (3.5.3.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6

The manner in which cryptographic keys are managed is a critical part of the continued security of the encryption solution. A good key-management process, whether it is manual or automated as part of the encryption product, is based on industry standards and addresses all key elements at 3.6.1 through 3.6.8.

Providing guidance to customers on how to securely transmit, store and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities.

This requirement applies to keys used to encrypt stored cardholder data, and any respective key-encrypting keys.

* 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. (3.6.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.1

The encryption solution must generate strong keys, as defined in the *PCI DSS* and *PA-DSS Glossary of Terms, Abbreviations, and Acronyms* under “Cryptographic Key Generation.” Use of strong cryptographic keys significantly increases the level of security of encrypted cardholder data. (3.6.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.2

The encryption solution must distribute keys securely, meaning the keys are distributed only to custodians identified in 3.5.1, and are never distributed in the clear.

Verify that key-management procedures specify how to securely distribute keys. (3.6.2.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.3

The encryption solution must store keys securely, for example, by encrypting them with a key-encrypting key. Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of cardholder data.

Verify that key-management procedures specify how to securely store keys. (3.6.3.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.4

A cryptoperiod is the time span during which a particular cryptographic key can be used for its defined purpose. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted.

Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimize the risk of someone’s obtaining the encryption keys, and using them to decrypt data.

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). (3.6.4.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.5

Keys that are no longer used or needed, or keys that are known or suspected to be compromised, should be revoked and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived, encrypted data) they should be strongly protected.

The encryption solution should provide for and facilitate a process to replace keys that are due for replacement or that are known to be, or suspected of being, compromised.

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 (3.6.5.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.6

Split knowledge and dual control of keys are used to eliminate the possibility of one person having access to the whole key. This control is applicable for manual key-management operations, or where key management is not implemented by the encryption product.

Split knowledge is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of the original cryptographic key.

Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another.

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 of keys) of another. (3.6.6.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.7

The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.

Verify that key-management procedures specify processes to prevent unauthorized substitution of keys. (3.6.7.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.6.8

This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities.

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. (3.6.8.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 3.7

Personnel need to be aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.

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.

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

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

### PCI-DSS Requirements 4.1

Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit.

Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted.

Note that some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates and supporting only strong encryption (not supporting weaker, insecure protocols or methods).

Verifying that certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection.

* 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. (4.1.a)
* 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. (4.1.b)

## Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

### PCI-DSS Requirements 4.1.1

Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks.

Strong cryptography for authentication and transmission of cardholder data is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data.

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. (4.1.1)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 4.2

E-mail, instant messaging, SMS, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. Do not utilize these messaging tools to send PAN unless they are configured to provide strong encryption.

Additionally, if an entity requests PAN via end-user messaging technologies, the entity should provide a tool or method to protect these PANs using strong cryptography or render PANs unreadable before transmission.

* Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. (4.2.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 4.3

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

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.

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

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

## PCI-DSS Requirements 5.1.1

It is important to protect against ALL types and forms of malicious software.

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
* Protect against all known types of malicious software

*Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.* (5.1.1)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 5.2

Even the best anti-virus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections.

Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. (5.2.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 5.4

Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

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. (5.4)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

# Requirement 6: Develop and maintain secure systems and applications

## PCI-DSS Requirements 6.1

The intent of this requirement is that organizations keep up to date with new vulnerabilities that may impact their environment.

Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing list, or RSS feeds.

Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. The organization must therefore have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities. This is not achieved by an ASV scan or internal vulnerability scan, rather this requires a process to actively monitor industry sources for vulnerability information.

Classifying the risks (for example, as “high,” “medium,” or “low”) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.

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 use reputable outside sources for security vulnerability information (6.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.2

There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data.

Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months.

This requirement applies to applicable patches for all installed software, including payment applications (both those that are PA-DSS validated and those that are not).

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). (6.2.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.3

Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment.

Understanding how sensitive data is handled by the application—including when stored, transmitted, and when in memory—can help identify where data needs to be protected.

* Examine written software-development processes to verify that the processes are based on industry standards and/or best practices. (6.3.a)
* Examine written software-development processes to verify that information security is included throughout the life cycle. (6.3.b)
* Examine written software-development processes to verify that software applications are developed in accordance with PCI DSS. (6.3.c)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.3.1

Development, test and/or custom application accounts, user IDs, and passwords should be removed from production code before the application becomes active or is released to customers, since these items may give away information about the functioning of the application. Possession of such information could facilitate compromise of the application and related cardholder data.

Examine written software-development procedures and interview responsible personnel to verify that preproduction and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. (6.3.1)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.3.2

Security vulnerabilities in custom code are commonly exploited by malicious individuals to gain access to a network and compromise cardholder data.

An individual knowledgeable and experienced in code-review techniques should be involved in the review process. Code reviews should be performed by someone other than the developer of the code to allow for an independent, objective review. Automated tools or processes may also be used in lieu of manual reviews, but keep in mind that it may be difficult or even impossible for an automated tool to identify some coding issues.

Correcting coding errors before the code is deployed into a production environment or released to customers prevents the code exposing the environments to potential exploit. Faulty code is also far more difficult and expensive to address after it has been deployed or released into production environments.

Including a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures.

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. (6.3.2.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.4

Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.

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.

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.4.1

Due to the constantly changing state of development and test environments, they tend to be less secure than the production environment. Without adequate separation between environments, it may be possible for the production environment, and cardholder data, to be compromised due to less-stringent security configurations and possible vulnerabilities in a test or development environment.

Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s). (6.4.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.4.5

If not properly managed, the impact of system changes—such as hardware or software updates and installation of security patches—might not be fully realized and could have unintended consequences.

Examine documented change control procedures and verify procedures are defined for:

* Documentation of impact
* Documented change 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.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.5

The application layer is high-risk and may be targeted by both internal and external threats.

Requirements 6.5.1 through 6.5.10 are the minimum controls that should be in place, and organizations should incorporate the relevant secure coding practices as applicable to the particular technology in their environment.

Application developers should be properly trained to identify and resolve issues related to these (and other) common coding vulnerabilities. Having staff knowledgeable of secure coding guidelines should minimize the number of security vulnerabilities introduced through poor coding practices. Training for developers may be provided in-house or by third parties and should be applicable for technology used.

As industry-accepted secure coding practices change, organizational coding practices and developer training should likewise be updated to address new threats—for example, memory scraping attacks.

The vulnerabilities identified in 6.5.1 through 6.5.10 provide a minimum baseline. It is up to the organization to remain up to date with vulnerability trends and incorporate appropriate measures into their secure coding practices.

* 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. (6.5.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.6

Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices.

* Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities
* Web-application firewalls filter and block non-essential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured. This can be achieved through a combination of technology and process. Process-based solutions must have mechanisms that facilitate timely responses to alerts in order to meet the intent of this requirement, which is to prevent attacks.

***Note:*** *“An organization that specializes in application security” can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*

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. (6.6)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 6.7

Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.

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. (6.7)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

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

## PCI-DSS Requirements 7.1

The more people who have access to cardholder data, the more risk there is that a user’s account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.

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. (7.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 7.2.1

Without a mechanism to restrict access based on user’s need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default “deny-all” setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.

***Note:*** *Some access control systems are set by default to “allow-all,” thereby permitting access unless/until a rule is written to specifically deny it.*

Confirm that access control systems are in place on all system components. (7.2.1)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 7.3

Personnel need to be aware of and following security policies and operational procedures to ensure that access is controlled and based on need-to-know and least privilege, on a continuous basis.

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. (7.3)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

# Requirement 8: Identify and authenticate access to system components

## PCI-DSS Requirements 8.1

By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.

Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8. (8.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.2

These authentication methods, when used in addition to unique IDs, help protect users’ IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Note that a digital certificate is a valid option for “something you have” as long as it is unique for a particular user.

Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.

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). (8.2)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.2.1

Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a “sniffer,” or directly access unencrypted passwords in files where they are stored, and use this data to gain unauthorized access.

Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage. (8.2.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.2.2

Many malicious individuals use "social engineering”—for example, calling a help desk and acting as a legitimate user—to have a password changed so they can utilize a user ID. Consider use of a “secret question” that only the proper user can answer to help administrators identify the user prior to re-setting or modifying authentication credentials.

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. (8.2.2)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.2.3

Strong passwords/passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID.

This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/ passphrases. For cases where this minimum cannot be met due to technical limitations, entities can use “equivalent strength” to evaluate their alternative. For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.)

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. (8.2.3.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.2.6

If the same password is used for every new user, an internal user, former employee, or malicious individual may know or easily discover this password, and use it to gain access to accounts.

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. (8.2.6)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.4

Communicating password/authentication policies and procedures to all users helps those users understand and abide by the policies.

For example, guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that don’t contain dictionary words, and that don’t contain information about the user (such as the user ID, names of family members, date of birth, etc.). Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files, and being alert for malicious individuals who may attempt to exploit their passwords (for example, by calling an employee and asking for their password so the caller can

“troubleshoot a problem”).

Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access.

* Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users. (8.4.a)
* 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 (8.4.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.5

If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This in turn prevents an entity from assigning accountability for, or having effective logging of, an individual’s actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.

Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. (8.5.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.5.1

To prevent the compromise of multiple customers through the use of a single set of credentials, vendors with remote access accounts to customer environments should use a different authentication credential for each customer.

Technologies, such as multi-factor mechanisms, that provide a unique credential for each connection (for example, via a single-use password) could also meet the intent of this requirement.

Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer.

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 8.6

If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through use of a shared authentication mechanism.

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. (8.6.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirement 8.8

Personnel need to be aware of and following security policies and operational procedures for managing identification and authorization on a continuous basis.

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. (8.8)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

# Requirement 9: Restrict physical access to cardholder data

## PCI-DSS Requirements 9.2

Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas containing cardholder data.

Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.

* Verify procedures 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.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.4.1

Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities (and potentially, to cardholder data).

Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.

Ensuring that visitor badges are returned upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.

A visitor log documenting minimum information on the visitor is easy and inexpensive to maintain and will assist in identifying physical access to a building or room, and potential access to cardholder data.

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. (9.4.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.5

Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any type of media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone’s desk.

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). (9.5)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.6

Procedures and processes help protect cardholder data on media distributed to internal and/or external users. Without such procedures, data can be lost or stolen and used for fraudulent purposes.

Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. (9.6)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.7

Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.

If media is not inventoried, stolen or lost media may not be noticed for a long time or at all.

Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. (9.7)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.8

If steps are not taken to destroy information contained on hard disks, portable drives,

CD/DVDs, or paper prior to disposal, malicious individuals may be able to retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trashcans and recycle bins looking for information they can use to launch an attack.

Securing storage containers used for materials that are going to be destroyed prevents sensitive information from being captured while the materials are being collected. For example, “to-be-shredded” containers could have a lock preventing access to its contents or physic ally prevent access to the inside of the container.

Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).

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). (9.8)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.9

Criminals attempt to steal cardholder data by stealing and/or manipulating card-reading devices and terminals. For example, they will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card information every time a card is entered. Criminals will also try to add “skimming” components to the outside of devices, which are designed to capture payment card details before they even enter the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card details are captured twice: once by the criminal’s component and then by the device’s legitimate component. In this way, transactions may still be completed without interruption while the criminal is “skimming” the payment card information during the process.

This requirement is recommended, but not required, for manual key-entry components such as computer keyboards and POS keypads.

Additional best practices on skimming prevention are available on the PCI SSC website.

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 devices (9.9)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.9.1

Keeping an up-to-date list of devices helps an organization keep track of where devices are supposed to be, and quickly identify if a device is missing or lost.

The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned.

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 (9.9.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.9.2

Regular inspections of devices will help organizations to more quickly detect tampering or replacement of a device, and thereby minimize the potential impact of using fraudulent devices.

The type of inspection will depend on the device—for example, photographs of devices that are known to be secure can be used to compare a device’s current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities. Device vendors may also be able to provide security guidance and “how to” guides to help determine whether the device has been tampered with.

The frequency of inspections will depend on factors such as location of device and whether the device is attended or unattended. For example, devices left in public areas without supervision by the organization’s personnel may have more frequent inspections than devices that are kept in secure areas or are supervised when they are accessible to the public. The type and frequency of inspections is determined by the merchant, as defined by their annual risk-assessment process.

Examine documented procedures to verify processes are defined to include the following:

* Procedures for inspecting devices
* Frequency of inspections

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

(9.9.2)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.10

Personnel need to be aware of and following security policies and operational procedures for restricting physical access to cardholder data and CDE systems on a continuous basis.

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. (9.10)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 9.9.3

Criminals will often pose as authorized maintenance personnel in order to gain access to POS devices. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POS maintenance company (such as the vendor or acquirer) for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work wear), and could also be knowledgeable about locations of devices, so it’s important personnel are trained to follow procedures at all times.

Another trick criminals like to use is to send a “new” POS system with instructions for swapping it with a legitimate system and “returning” the legitimate system to a specified address. The criminals may even provide return postage as they are very keen to get their hands on these devices. Personnel always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business.

Review training materials for personnel at point-of-sale locations to verify they 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 suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer) (9.9.3.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

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

## PCI-DSS Requirements 10.4

Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.

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. (10.4)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 10.6.1

Checking logs daily minimizes the amount of time and exposure of a potential breach.

Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that the determination of “security event” will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of “normal” traffic to help identify anomalous behavior.

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.) (10.6.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 10.6.2

Logs for all other system components should also be periodically reviewed to identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems. The frequency of the reviews should be determined by an entity’s annual risk assessment.

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. (10.6.2.a)

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. (10.6.2.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 10.6.3

If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.

Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. (10.6.3.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 10.7

Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.

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. (10.7.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 10.8

Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.

The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.

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) (10.8.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 10.8.1

If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity’s environment.

Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.

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 (10.8.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 10.9

Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.

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. (10.9)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

# Requirement 11: Regularly test security systems and processes

## PCI-DSS Requirements 11.1

Implementation and/or exploitation of wireless technology within a network are some of the most common paths for malicious users to gain access to the network and cardholder data. If a wireless device or network is installed without a company’s knowledge, it can allow an attacker to easily and “invisibly” enter the network. Unauthorized wireless devices may be hidden within or attached to a computer or other system component, or be attached directly to a network port or network device, such as a switch or router. Any such unauthorized device could result in an unauthorized access point into the environment.

Knowing which wireless devices are authorized can help administrators quickly identify non-authorized wireless devices, and responding to the identification of unauthorized wireless access points helps to proactively minimize the exposure of CDE to malicious individuals.

Due to the ease with which a wireless access point can be attached to a network, the difficulty in detecting their presence, and the increased risk presented by unauthorized wireless devices, these processes must be performed even when a policy exists prohibiting the use of wireless technology.

The size and complexity of a particular environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment.

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. (11.1.a)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 11.1.2

Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found. (11.1.2.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 11.3

The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks.

A penetration test differs from a vulnerability scan, as a penetration test is an active process that may include exploiting identified vulnerabilities. Conducting a vulnerability scan may be one of the first steps a penetration tester will perform in order to plan the testing strategy, although it is not the only step. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps.

Penetration testing is generally a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to penetrate into an environment. Often the tester will chain several types of exploits together with a goal of breaking through layers of defenses. For example, if the tester finds a means to gain access to an application server, they will then use the compromised server as a point to stage a new attack based on the resources the server has access to. In this way, a tester is able to simulate the methods performed by an attacker to identify areas of potential weakness in the environment.

Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes 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
* 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 6.5Defines 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)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 11.4

Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known “signatures” and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.

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. (11.4.c)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 11.6

Personnel need to be aware of and following security policies and operational procedures for security monitoring and testing on a continuous basis.

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. (11.6)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

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

## PCI-DSS Requirements 12.1

A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). (12.1)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 12.2

A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business. Examples of different risk considerations include cybercrime, web attacks, and POS malware. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized.

Performing risk assessments at least annually and upon significant changes allows the organization to keep up to date with organizational changes and evolving threats, trends, and technologies.

Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. (12.2.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 12.3

Personnel usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for personnel as to correct usage and implementation. If usage policies are not in place, personnel may use the technologies in violation of company policy, thereby allowing malicious individuals to gain access to critical systems and cardholder data.

Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed:

* Documented,
* In use, and
* Known to all affected parties. (12.3.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 12.4.1

Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.

Examine documentation to verify executive management has assigned overall accountability for maintaining the entity’s PCI DSS compliance. (12.4.1.a)

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. (12.4.1.b)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 12.5

Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data.

Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.

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. (12.5)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 12.6

If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.

Examine security awareness program procedures and documentation and perform the following: (12.6.b)

* 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) (12.6.1.a)
* Verify that personnel attend security awareness training upon hire and at least annually (12.6.1.b)
* Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security (12.6.1.c)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 12.8

If a merchant or service provider shares cardholder data with a service provider, certain requirements apply to ensure continued protection of this data will be enforced by such service providers.

Some examples of the different types of service providers include backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, entities that receive data for fraud-modeling purposes, etc.

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:

(12.8)

### Procedure

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus est, eleifend id sem accumsan, euismod ultricies dui. Proin fermentum nibh enim, eu lacinia orci accumsan et. Sed lacus turpis, sagittis nec mauris eu, semper accumsan magna.

## PCI-DSS Requirements 12.8.3

The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider.

Specific due-diligence processes and goals will vary for each organization. Examples of considerations may include the provider’s reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider validates their PCI DSS compliance and what evidence they will provide, etc.

Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider.

### Procedure

## PCI-DSS Requirements 12.9

### Procedure

## PCI-DSS Requirements 12.10

### Procedure

## PCI-DSS Requirements 12.10.2

### Procedure

## PCI-DSS Requirements 12.10.3

### Procedure

## PCI-DSS Requirements 12.10.4

### Procedure

## PCI-DSS Requirements 12.10.6

### Procedure

## PCI-DSS Requirements 12.11

(12.11.a)

(12.11.b)

### Procedure

## PCI-DSS Requirements 12.11.1

(12.11.1.a)

### Procedure