## GLBA Safeguards Rule

### General Requirements

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

### Employee Management and Training

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

### Information Systems

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

### Detecting and Managing System Failures

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