Mapping PCI DSS 3.0 to Instant PCI Policy

Below are the requirements from the PCI Data Security Standard, **version 3.0**. Each requirement is followed by a bullet point that tells exactly where that requirement is covered by your Instant PCI Policy. Refer to www.InstantSecurityPolicy.com for more information.

Please note that, as with any regulation or security standard, the procedures you put into place to enforce your policies are critical to your compliance.

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

1.1 Establish and implement firewall and router configuration standards that include the following:

1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware
- Network Security Policy, 4.17 Change Management

1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks

- Network Security Policy, 4.12 Network Documentation

1.1.3 Current diagram that shows all cardholder data flows across systems and networks

- Network Security Policy, 4.12 Network Documentation

1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

- Network Security Policy, 4.4 Firewalls
- Network Security Policy, 4.11 Network Compartmentalization

1.1.5 Description of groups, roles, and responsibilities for management of network components

- Network Security Policy, 4.21 Security Policy Management

1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration

1.1.7 Requirement to review firewall and router rule sets at least every six months

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

- Confidential Data Policy, 4.7 Security Controls for Confidential Data
- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.11 Network Compartmentalization, 4.11.1 High Risk Networks and High Security Zones

1.2.2 Secure and synchronize router configuration files.

- Network Security Policy, 4.5 Networking Hardware

1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

- Wireless Access Policy, 4.3 Access Confidential Data
- Network Security Policy, 4.11 Network Compartmentalization, 4.11.1 High Risk Networks and High Security Zones

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

- Confidential Data Policy, 4.7 Security Controls for Confidential Data
- Network Security Policy, 4.11 Network Compartmentalization, 4.11.1 High Risk Networks and High Security Zones

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.

- Network Security Policy, 4.11 Network Compartmentalization, 4.11.1 High Risk Networks and High Security Zones

1.3.4 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware

1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

- Network Security Policy, 4.11 Network Compartmentalization, 4.11.1 High Risk Networks and High Security Zones
- Network Security Policy, 4.4 Firewalls, 4.4.2 Outbound Traffic Filtering

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)

- Network Security Policy, 4.11 Network Compartmentalization, 4.11.1 High Risk Networks and High Security Zones

1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

- Confidential Data Policy, 4.7 Security Controls for Confidential Data
- Network Security Policy, 4.11 Network Compartmentalization, 4.11.1 High Risk Networks and High Security Zones

1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware
- Network Security Policy, 4.6 Network Servers

1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include:

- Specific configuration settings are defined for personal firewall software.
- Personal firewall software is actively running.
- Personal firewall software is not alterable by users of mobile and/or employee-owned devices.

- Remote Access Policy, 4.1 Remote Access Client Software
- Mobile Device Policy, 4.3 Connecting Mobile Computers to Unsecured Networks

1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

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

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.

This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, *point-of-sale* (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.

- Network Security Policy, 4.1 Network Device Authentication, 4.1.3 Network Device Default Value Change Requirements

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

- Network Security Policy, 4.1 Network Device Authentication, 4.1.3 Network Device Default Value Change Requirements
- Wireless Access Policy, 4.2 Configuration and Installation, 4.2.2 Installation

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

Sources of industry-accepted system hardening standards may include, but are not limited to:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Network Hardware
- Network Security Policy, 4.6 Network Servers

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

- Network Security Policy, 4.6 Network Servers

2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Network Hardware
- Network Security Policy, 4.6 Network Servers

2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

- Network Security Policy, 4.5 Networking Hardware
- Network Security Policy, 4.6 Network Servers

2.2.4 Configure system security parameters to prevent misuse.

- Network Security Policy, 4.6 Network Servers

2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

- Network Security Policy, 4.6 Network Servers

2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

- Remote Access Policy, 4.2 Remote Network Access, 4.2.2 Administrators

2.4 Maintain an inventory of system components that are in scope for PCI DSS.

- Network Security Policy, 4.12 Network Documentation

2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*

- Confidential Data Policy, 4.6 Receiving Confidential Data from Third Parties

Requirement 3: Protect stored cardholder data

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements
- Processes for secure deletion of data when no longer needed
- Specific retention requirements for cardholder data
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

- Retention Policy, 4.3 Retention Requirements
- Retention Policy, 4.5 Data Destruction
- Network Security Policy, 4.10 Disposal of Information Technology Assets

3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.1 Storage

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.1 Storage

3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not present transactions.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.1 Storage

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.1 Storage

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.

- Confidential Data Policy, 4.7 Security Controls for Confidential Data

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.1 Storage

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system authentication and access

control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

- , 4.1 Applicability of Encryption, 4.1.7 Confidential Data

3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.

- Encryption Policy, 4.2 Encryption Key Management

3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.

- Encryption Policy, 4.2 Encryption Key Management

3.5.2 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key
- Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point of interaction device)
- As at least two full-length key components or key shares, in accordance with an industry-accepted method

- Encryption Policy, 4.2 Encryption Key Management

3.5.3 Store cryptographic keys in the fewest possible locations.

- Encryption Policy, 4.2 Encryption Key Management

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:

3.6.1 Generation of strong cryptographic keys

- Encryption Policy, 4.3 Acceptable Encryption Algorithms

3.6.2 Secure cryptographic key distribution

- Encryption Policy, 4.2 Encryption Key Management

3.6.3 Secure cryptographic key storage

- Encryption Policy, 4.2 Encryption Key Management

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

- Encryption Policy, 4.2 Encryption Key Management

3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.

- Network Security Policy, 4.1 Network Device Authentication, 4.1.3 Network Device Default Value Change Requirements

3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control.

- Encryption Policy, 4.2 Encryption Key Management

3.6.7 Prevention of unauthorized substitution of cryptographic keys.

- Encryption Policy, 4.2 Encryption Key Management

3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

- Encryption Policy, 4.2 Encryption Key Management

3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

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

4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:

- Only trusted keys and certificates are accepted
- The protocol in use only supports secure versions or configurations
- The encryption strength is appropriate for the encryption methodology in use.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.2 Transmission
- Confidential Data Policy, 4.7 Security Controls for Confidential Data

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.2 Transmission
- Confidential Data Policy, 4.7 Security Controls for Confidential Data
- Wireless Access Policy, 4.3 Accessing Confidential Data

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

- Acceptable Use Policy, 4.2 Web Browsing and Internet Usage, 4.2.5 Instant Messaging
- Email Policy, 4.3 Confidential Data and Email, 4.3.3 Emailing Cardholder Data

4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

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

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

- Network Security Policy, 4.13 Antivirus/Anti-Malware

5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

- Network Security Policy, 4.13 Antivirus/Anti-Malware

5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

- Network Security Policy, 4.13 Antivirus/Anti-Malware

5.2 Ensure that all anti-virus mechanisms are maintained as follows:
- Are kept current
- Perform periodic scans
- Generate audit logs which are retained per PCI DSS Requirement 10.7

- Network Security Policy, 4.13 Antivirus/Anti-Malware

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

- Network Security Policy, 4.13 Antivirus/Anti-Malware

5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

Requirement 6: Develop and maintain secure systems and applications

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

- Network Security Policy, 4.14 Software Use Policy

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

- Network Security Policy, 4.14 Software Use Policy

6.3 Develop internal and external software applications (including a web-based administrative access to applications) securely, as follows:
- In accordance with PCI DSS (for example, secure authentication and logging)
- Based on industry standards and/or best practices
- Incorporating information security throughout the software-development life cycle

- Network Security Policy, 4.15 Software/Application Development Policy

6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.

- Network Security Policy, 4.15 Software/Application Development Policy

6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:

- Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines
- Appropriate corrections are implemented prior to release.
- Code-review results are reviewed and approved by management prior to release.

- Network Security Policy, 4.15 Software/Application Development Policy

6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:

6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.

- Network Security Policy, 4.15 Software/Application Development Policy

6.4.2 Separation of duties between development/test and production environments

- Network Security Policy, 4.15 Software/Application Development Policy

6.4.3 Production data (live PANs) are not used for testing or development

- Network Security Policy, 4.15 Software/Application Development Policy

6.4.4 Removal of test data and accounts before production systems become active

- Network Security Policy, 4.15 Software/Application Development Policy

6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:

6.4.5.1 Documentation of impact.

- Network Security Policy, 4.15 Software/Application Development Policy

6.4.5.2 Documented change approval by authorized parties.

- Network Security Policy, 4.15 Software/Application Development Policy

6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.

- Network Security Policy, 4.15 Software/Application Development Policy

6.4.5.4 Back-out procedures.

- Network Security Policy, 4.15 Software/Application Development Policy

6.5 Address common coding vulnerabilities in software-development processes as follows:
- Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.
- Develop applications based on secure coding guidelines.

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.2 Buffer overflows

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.3 Insecure cryptographic storage

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.4 Insecure communications

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.5 Improper error handling

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.7 Cross-site scripting (XSS)

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal, and failure to restrict user access to functions).

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.9 Cross-site request forgery (CSRF)

- Network Security Policy, 4.15 Software/Application Development Policy

6.5.10 Broken authentication and session management

- Network Security Policy, 4.15 Software/Application Development Policy

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

- Network Security Policy, 4.15 Software/Application Development Policy

6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

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

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

- Network Access and Authentication Policy, 4.2 Account Access Levels
- External Connection Policy, 4.3 Implementation

7.1.1 Define access needs for each role, including:
- System components and data resources that each role needs to access for their job function
- Level of privilege required (for example, user, administrator, etc.) for accessing resources.

- Network Access and Authentication Policy, 4.2 Account Access Levels
- External Connection Policy, 4.3 Implementation

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

- Network Access and Authentication Policy, 4.2 Account Access Levels

7.1.3 Assign access based on individual personnel's job classification and function.

- Network Access and Authentication Policy, 4.2 Account Access Levels

7.1.4 Require documented approval by authorized parties specifying required privileges.

- Network Access and Authentication Policy, 4.5 Network Authentication Requests

7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

- Network Access and Authentication Policy, 4.2 Account Access Levels

This access control system must include the following:

7.2.1 Coverage of all system components

- Network Access and Authentication Policy, 4.2 Account Access Levels

7.2.2 Assignment of privileges to individuals based on job classification and function

- Network Access and Authentication Policy, 4.2 Account Access Levels

7.2.3 Default “deny-all” setting

- Network Access and Authentication Policy, 4.2 Account Access Levels

7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

Requirement 8: Identify and authenticate access to system components

8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:

8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

- Network Access and Authentication Policy, 4.1 Account Setup

8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

- Network Access and Authentication Policy, 4.1 Account Setup

8.1.3 Immediately revoke access for any terminated users.

- Network Access and Authentication Policy, 4.4 Account Termination

8.1.4 Remove/disable inactive user accounts at least every 90 days.

- Network Access and Authentication Policy, 4.4 Account Termination

8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:
- Enabled only during the time period needed and disabled when not in use.
- Monitored when in use.

- Network Access and Authentication Policy, 4.3 Account Use

8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.

- Network Access and Authentication Policy, 4.11 Failed Login Attempts

8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

- Network Access and Authentication Policy, 4.11 Failed Login Attempts

8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

- Network Access and Authentication Policy, 4.5 Network Authentication Requests
- Remote Access Policy, 4.3 Idle Connections

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric.

- Network Access and Authentication Policy, 4.3 Account Use

8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

- Network Access and Authentication Policy, 4.10 Encryption of Login Credentials

8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.

- Network Access and Authentication Policy, 4.1 Account Setup

8.2.3 Passwords/phrases must meet the following:

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.

- Password Policy, 4.1 Construction

8.2.4 Change user passwords/passphrases at least every 90 days.

- Password Policy, 4.3 Change Frequency

8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.

- Password Policy, 4.3 Change Frequency
- Network Access and Authentication Policy, 4.7 Use of Passwords

8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.

- Password Policy, 4.1 Construction

8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).

- Remote Access Policy, 4.2 Remote Network Access

8.4 Document and communicate authentication procedures and policies to all users including:
- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

- Password Policy, 4.1 Construction
- Password Policy, 4.2 Confidentiality
- Password Policy, 4.3 Change Frequency
- Password Policy, 4.4 Incident Reporting

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:
- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

- Network Access and Authentication Policy, 4.3 Account Use

8.5.1 ***Additional requirement for service providers:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

- Network Access and Authentication Policy, 4.3 Account Use

8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:

- Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
- Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

- Network Access and Authentication Policy, 4.12 Alternate Authentication Mechanisms

8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods.
- Only database administrators have the ability to directly access or query databases.
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

- Network Access and Authentication Policy, 4.6 Database Authentication Requests

8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

Requirement 9: Restrict physical access to cardholder data

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

(See below)

9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

- Physical Security Policy, 4.2 Security Zones, 4.2.3 Private

9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks.

- Physical Security Policy, 4.4 Physical Data Security

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

- Wireless Access Policy, 4.1 Physical Guidelines
- Physical Security Policy, 4.4 Physical Data Security
- Physical Security Policy, 4.5 Physical Systems Security, 4.5.1 Minimizing Risk of Loss or Theft

9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include:

- Identifying new onsite personnel or visitors (for example, assigning badges)
- Changes to access requirements
- Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).

- Physical Security Policy, 4.7 Entry Security, 4.7.1 Use of Identification Badges

9.3 Control physical access for onsite personnel to the sensitive areas as follows:

- Access must be authorized and based on individual job function.
- Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

- Physical Security Policy, 4.2 Security Zones, 4.2.3 Private
- Physical Security Policy, 4.7 Entry Security, 4.7.4 Termination

9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:

9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.

- Physical Security Policy, 4.7 Entry Security, 4.7.3 Visitor Access

9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.

- Physical Security Policy, 4.7 Entry Security, 4.7.1 Use of Identification Badges

9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.

- Physical Security Policy, 4.7 Entry Security, 4.7.1 Use of Identification Badges

9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.

- Physical Security Policy, 4.7 Entry Security, 4.7.2 Sign-in Requirements

9.5 Physically secure all media.

- Physical Security Policy, 4.4 Physical Data Security

9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.

- Backup Policy, 4.5 Backup Storage

9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:

9.6.1 Classify media so the sensitivity of the data can be determined.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.1 Storage

9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.

- Confidential Data Policy, 4.5 Sharing Confidential Data with Third Parties

9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).

- Confidential Data Policy, 4.7 Security Controls for Confidential Data

9.7 Maintain strict control over the storage and accessibility of media.

- Confidential Data Policy, 4.7 Security Controls for Confidential Data

9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.

- Confidential Data Policy, 4.7 Security Controls for Confidential Data

9.8 Destroy media when it is no longer needed for business or legal reasons as follows:

9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.3 Destruction

9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.3 Destruction

9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

- Physical Security Policy, 4.5 Physical System Security, 4.5.3 Minimizing Risk of Tampering

9.9.1 Maintain an up-to-date list of devices. The list should include the following:
- Make, model of device
- Location of device (for example, the address of the site or facility where the device is located)
- Device serial number or other method of unique identification.

- Physical Security Policy, 4.5 Physical System Security, 4.5.3 Minimizing Risk of Tampering

9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

- Physical Security Policy, 4.5 Physical System Security, 4.5.3 Minimizing Risk of Tampering

9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:
- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

- Physical Security Policy, 4.5 Physical System Security, 4.5.3 Minimizing Risk of Tampering

9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

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

10.1 Implement audit trails to link all access to system components to each individual user.

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process
- Network Security Policy, 4.3 Audit Trails, 4.3.2 What to Record
- Network Security Policy, 4.3 Audit Trails, 4.3.3 Security of Audit Trails

10.2 Implement automated audit trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.2.2 All actions taken by any individual with root or administrative privileges

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.2.3 Access to all audit trails

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.2.4 Invalid logical access attempts

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.2.6 Initialization, stopping, or pausing of the audit logs

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.2.7 Creation and deletion of system-level objects

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.3 Record at least the following audit trail entries for all system components for each event:

10.3.1 User identification

- Network Security Policy, 4.3 Audit Trails, 4.3.2 What to Record

10.3.2 Type of event

- Network Security Policy, 4.3 Audit Trails, 4.3.2 What to Record

10.3.3 Date and time

- Network Security Policy, 4.3 Audit Trails, 4.3.2 What to Record

10.3.4 Success or failure indication

- Network Security Policy, 4.3 Audit Trails, 4.3.2 What to Record

10.3.5 Origination of event

- Network Security Policy, 4.3 Audit Trails, 4.3.2 What to Record

10.3.6 Identity or name of affected data, system component, or resource.

- Network Security Policy, 4.3 Audit Trails, 4.3.2 What to Record

10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware
- Network Security Policy, 4.6 Network Servers

10.4.1 Critical systems have the correct and consistent time.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware
- Network Security Policy, 4.6 Network Servers

10.4.2 Time data is protected.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware
- Network Security Policy, 4.6 Network Servers

10.4.3 Time settings are received from industry-accepted time sources.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration
- Network Security Policy, 4.5 Networking Hardware
- Network Security Policy, 4.6 Network Servers

10.5 Secure audit trails so they cannot be altered.

- Network Security Policy, 4.3 Audit Trails, 4.3.3 Security of Audit Trails

10.5.1 Limit viewing of audit trails to those with a job-related need.

- Network Security Policy, 4.3 Audit Trails, 4.3.3 Security of Audit Trails

10.5.2 Protect audit trail files from unauthorized modifications.

- Network Security Policy, 4.3 Audit Trails, 4.3.3 Security of Audit Trails

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

- Network Security Policy, 4.3 Audit Trails, 4.3.3 Security of Audit Trails

10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

- Network Security Policy, 4.3 Audit Trails, 4.3.3 Security of Audit Trails

10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

- Network Security Policy, 4.3 Audit Trails, 4.3.3 Security of Audit Trails

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

- Network Security Policy, 4.2 Logging, 4.2.2 Log Review

10.6.1 Review the following at least daily:
- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD, 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 (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

- Network Security Policy, 4.2 Logging, 4.2.2 Log Review

10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.

- Network Security Policy, 4.2 Logging, 4.2.2 Log Review

10.6.3 Follow up exceptions and anomalies identified during the review process.

- Network Security Policy, 4.2 Logging, 4.2.2 Log Review

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).

- Network Security Policy, 4.3 Audit Trails, 4.3.1 Audit Trail Process

10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

Requirement 11: Regularly test security systems and processes.

11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

- Network Security Policy, 4.9 Security Testing, 4.9.1 Wireless Scans

11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.

- Wireless Access Policy, 4.7 Wireless Access Point Inventory

11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.

- Incident Response Policy, 4.6 Hybrid Incidents

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

(see below)

11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.

- Network Security Policy, 4.9 Security Testing, 4.9.2 Internal Vulnerability Scans

11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

- Network Security Policy, 4.9 Security Testing, 4.9.3 External Vulnerability Scans

11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.

- Network Security Policy, 4.9 Security Testing, 4.9.2 Internal Vulnerability Scans
- Network Security Policy, 4.9 Security Testing, 4.9.3 External Vulnerability Scans

11.3 Implement a methodology for penetration testing 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
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5

- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

- Network Security Policy, 4.9 Security Testing, 4.9.4 Penetration Testing

11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

- Network Security Policy, 4.9 Security Testing, 4.9.4 Penetration Testing

11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

- Network Security Policy, 4.9 Security Testing, 4.9.4 Penetration Testing

11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

- Network Security Policy, 4.9 Security Testing, 4.9.4 Penetration Testing

11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

- Network Security Policy, 4.7 Intrusion Detection/Intrusion Prevention

11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

- Network Security Policy, 4.8 File Integrity Monitoring

11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.

- Network Security Policy, 4.8 File Integrity Monitoring

11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

- Network Security Policy, 4.12 Network Documentation

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

12.1 Establish, publish, maintain, and disseminate a security policy.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.1.1 Review the security policy at least annually and update the policy when the environment changes.

- Network Security Policy, 4.21 Security Policy Management

12.2 Implement a risk-assessment process that:
- Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),
- Identifies critical assets, threats, and vulnerabilities, and
- Results in a formal risk assessment.

- Incident Response Policy, 4.8 Managing Risk, 4.8.1 Risk Assessment & 4.8.2 Risk Management Program

12.3 Develop usage policies for critical technologies and define proper use of these technologies.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

Ensure these usage policies require the following:

12.3.1 Explicit approval by authorized parties

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.3.2 Authentication for use of the technology

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.3.3 A list of all such devices and personnel with access

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)

- Network Security Policy, 4.17 Change Management

12.3.5 Acceptable uses of the technology

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.3.6 Acceptable network locations for the technologies

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.3.7 List of company-approved products

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity

- Remote Access Policy, 4.3 Idle Connections

12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use

- Remote Access Policy, 4.2 Remote Network Access, 4.2.3 Third Parties/Vendors

12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.

Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

- Mobile Device Policy, 4.4 General Guidelines
- Remote Access Policy, 4.4 Prohibited Actions

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.5 Assign to an individual or team the following information security management responsibilities:

(See below)

12.5.1 Establish, document, and distribute security policies and procedures.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.5.4 Administer user accounts, including additions, deletions, and modifications

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.5.5 Monitor and control all access to data.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.

- Network Security Policy, 4.21 Security Policy Management 4.21.2 Security Awareness Training

12.6.1 Educate personnel upon hire and at least annually.

- Network Security Policy, 4.21 Security Policy Management, 4.21.2 Security Awareness Training

12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.

- Network Security Policy, 4.21 Security Policy Management, 4.21.2 Security Awareness Training

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)

- Network Access and Authentication Policy, 4.1 Account Setup

12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

12.8.1 Maintain a list of service providers.

- Outsourcing Policy, 4.7 List of Providers

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

- Confidential Data Policy, 4.5 Sharing Confidential Data with Third Parties

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

- Outsourcing Policy, 4.3 Evaluating a Provider

12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

- Outsourcing Policy, 4.3 Evaluating a Provider

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

- Outsourcing Policy, 4.7 List of Providers

12.9 ***Additional requirement for service providers*****:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

- Confidential Data Policy, 4.6 Receiving Confidential Data from Third Parties

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.

- Incident Response Policy (in whole)

12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response procedures from the payment brands.

- Incident Response Policy (in whole)
- Backup Policy (in whole)

12.10.2 Test the plan at least annually.

- Incident Response Policy, 4.8 Managing Risk

12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.10.4 Provide appropriate training to staff with security breach response responsibilities.

- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager
- Network Security Policy, 4.21 Security Policy Management, 4.21.2 Security Awareness Training
- Acceptable Use Policy, 4.7 Reporting of a Security Incident

12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

- Incident Response Policy, 4.1 Types of Incidents, 4.1.1 Electronic
- Wireless Access Policy, 4.5 Wireless Scans
- Network Security Policy, 4.7 Intrusion Detection/Intrusion Prevention
- Network Security Policy, 4.8 File Integrity Monitoring
- Network Security Policy 4.9 Security Testing
- Network Security Policy, 4.21 Security Policy Management, 4.21.1 Information Security Manager

12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

- Incident Response Policy, 4.4 Electronic Incidents
- Incident Response Policy, 4.5 Physical Incidents
- Incident Response Policy, 4.6 Hybrid Incidents
- Incident Response Policy, 4.8 Managing Risk, 4.8.2 Risk Management Program