Mapping PCI DSS 2.0 to Instant PCI Policy

Below are the requirements from the PCI Data Security Standard, version 2.0. 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 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 with all connections to cardholder data, including any wireless networks

- Network Security Policy, 4.12 Network Documentation

1.1.3 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

1.1.4 Description of groups, roles, and responsibilities for logical management of network components

- Network Security Policy, 4.21 Security Policy Management

1.1.5 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.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration

1.1.6 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.

(See below)

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

- Confidential Data Policy, 4.6 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

1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

- Wireless Access Policy, 4.2 Configuration and Installation, 4.2.1 Security Configuration
- 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

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

- Confidential Data Policy, 4.6 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 Do not allow internal addresses to pass from the Internet into the DMZ.

- Network Security Policy, 4.4 Firewalls, 4.4.1 Configuration

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.

- 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, 4.6 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 computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

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

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

2.1 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

- 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 wireless vendor defaults, 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.

- 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 and secure services, protocols, daemons, etc., as required for the function of the system. Implement 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

2.2.3 Configure system security parameters to prevent misuse.

- Network Security Policy, 4.6 Network Servers

2.2.4 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 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.*

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, as follows.

3.1.1 Implement a data retention and disposal policy that includes:

_ 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 automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements

- 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).

- 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).

- Confidential Data Policy, 4.6 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 access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.

- Encryption Policy, 4.1 Applicability of Encryption, 4.1.7 Confidential Data

3.5 Protect any keys used to secure cardholder data against disclosure and misuse:

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 cryptographic keys securely in the fewest possible locations and forms.

- 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 ciphertext 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), 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 (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).

- 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

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.

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.2 Transmission
- Confidential Data Policy, 4.6 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. ***Note:*** *The use of WEP as a security control was prohibited as of 30 June 2010.*

- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.2 Transmission
- Confidential Data Policy, 4.6 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

Requirement 5: Use 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

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

- Network Security Policy, 4.13 Antivirus/Anti-Malware

Requirement 6: Develop and maintain secure systems and applications

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

- Network Security Policy, 4.14 Software Use Policy

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

- Network Security Policy, 4.14 Software Use Policy

6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:

- Network Security Policy, 4.15 Software/Application Development Policy

6.3.1 Removal of 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 of custom code prior to release to production or customers in order to identify any potential coding vulnerability.

- 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 and production environments

- 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. Procedures 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 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:

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 overflow

- 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" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).

- 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)

- 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

6.6 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 a web-application firewall in front of public-facing web applications

- Network Security Policy, 4.15 Software/Application Development Policy

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. Access limitations must include the following:

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

7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities

- Network Access and Authentication Policy, 4.2 Account Access Levels

- External Connection Policy, 4.3 Implementation

7.1.2 Assignment of privileges is based on individual personnel's job classification and function

- Network Access and Authentication Policy, 4.2 Account Access Levels

7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.

- Network Access and Authentication Policy, 4.2 Account Access Levels

7.1.4 Implementation of an automated access control system

- Network Access and Authentication Policy, 4.5 Authentication

7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:

7.2.1 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

Requirement 8: Assign a unique ID to each person with computer access

8.1 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
- Network Access and Authentication Policy, 4.3 Account Use

8.2 In addition to assigning a unique ID**,** employ 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

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)

- Remote Access Policy, 4.2 Remote Network Access

8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.

- Network Access and Authentication Policy, 4.9 Encryption of Login Credentials
- Confidential Data Policy, 4.2 Treatment of Confidential Data, 4.2.1 Storage

8.5 Ensure proper user identification and authentication management for nonconsumer users and administrators on all system components as follows:

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

- Network Access and Authentication Policy, 4.1 Account Setup

8.5.2 Verify user identity before performing password resets.

- Network Access and Authentication Policy, 4.1 Account Setup

8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.

- Network Access and Authentication Policy, 4.1 Account Setup

8.5.4 Immediately revoke access for any terminated users.

- Network Access and Authentication Policy, 4.4 Account Termination

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

- Network Access and Authentication Policy, 4.4 Account Termination

8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.

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

8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.

- Network Access and Authentication Policy, 4.1 Account Setup

8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.

- Network Access and Authentication Policy, 4.3 Account Use

8.5.9 Change user passwords at least every 90 days.

- Password Policy, 4.3 Change Frequency
- Network Access and Authentication Policy, 4.6 Use of Passwords

8.5.10 Require a minimum password length of at least seven characters.

- Password Policy, 4.1 Construction

8.5.11 Use passwords containing both numeric and alphabetic characters.

- Password Policy, 4.1 Construction

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

- Network Access and Authentication Policy, 4.6 Use of Passwords

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

- Network Access and Authentication Policy, 4.10 Failed Login Attempts

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

- Network Access and Authentication Policy, 4.10 Failed Login Attempts

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

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

8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.

- Network Access and Authentication, 4.5 Authentication

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 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.

- 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, especially in areas where cardholder data is accessible.

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

9.3 Make sure all visitors are handled as follows:

9.3.1 Authorized before entering areas where cardholder data is processed or maintained.

- Physical Security Policy, 4.7 Entry Security, 4.7.2 Sign-in Requirements, 4.7.3 Visitor Access

9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.

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

9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.

- Physical Security Policy, 4.7 Entry Security, 4.7.1 Use of Identification Badges
- Physical Security Policy, 4.7 Entry Security, 4.7.3 Visitor Access

9.4 Use a visitor log to maintain a physical audit trail of visitor activity. 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 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back up site, or a commercial storage facility. Review the location's security at least annually.

- Backup Policy, 4.5 Backup Storage

9.6 Physically secure all media.

- Physical Security Policy, 4.4 Physical Data Security

9.7 Maintain strict control over the internal or external distribution of any kind of media.

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

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

- Confidential Data Policy, 4.1 Data Classification

9.7.2 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

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

- Confidential Data Policy, 4.6 Security Controls for Confidential Data

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

- Confidential Data Policy, 4.6 Security Controls for Confidential Data

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

- Confidential Data Policy, 4.6 Security Controls for Confidential Data

9.10 Destroy media when it is no longer needed for business or legal reasons.

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

9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

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

9.10.2 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

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

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) 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 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 identification and authentication mechanisms

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

10.2.6 Initialization 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 log server on the internal LAN.

- 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 for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

- 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 back-up).

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

Requirement 11: Regularly test security systems and processes.

11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

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

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.

- 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).

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

11.2.3 Perform internal and external scans after any significant change.

- 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 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a subnetwork added to the environment, or a web server added to the environment). These penetration tests must include the following:

11.3.1 Network-layer penetration tests

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

11.3.2 Application-layer penetration tests

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

11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of 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 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

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

12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

- Network Security Policy, 4.21 Security Policy Management

12.1.1 Addresses all PCI DSS requirements.

- Covered by policy in whole

12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)

- Incident Response Policy, 4.7 Managing Risk, 4.7.1 Risk Assessment & 4.7.2 Risk Management Program

12.1.3 Includes a review at least annually and updates when the environment changes.

- Network Security Policy, 4.21 Security Policy Management 4.21.3 Security Policy Review

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

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

12.3 Develop usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. 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 Labeling of devices to determine owner, contact information and purpose

- 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 copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.

- 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 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:

(See below)

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.

- 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

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

- Covered by Incident Response Plan in whole

12.9.1 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

- Incident Response Policy, 4.2 Preparation

_ Specific incident response procedures

- Incident Response Policy, 4.4 Electronic Incidents and 4.5 Physical Incidents

_ Business recovery and continuity procedures

- Incident Response Policy, 4.4 Electronic Incidents and 4.5 Physical Incidents

_ Data back-up processes

- Incident Response Policy, 4.4 Electronic Incidents and 4.5 Physical Incidents
- Backup Policy (in whole)

_ Analysis of legal requirements for reporting compromises

- Incident Response Policy, 4.4 Electronic Incidents and 4.5 Physical Incidents

_ Coverage and responses of all critical system components

- Incident Response Policy (plan in whole)

_ Reference or inclusion of incident response procedures from the payment brands

- Incident Response Policy, 4.2 Preparation

12.9.2 Test the plan at least annually.

- Incident Response Policy, 4.7 Managing Risk

12.9.3 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

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

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

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

- Incident Response Policy, 4.1 Types of Incidents, 4.1.1 Electronic

12.9.6 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, 4.5.1 Response
- Incident Response Policy, 4.7 Managing Risk, 4.7.2 Risk Management Program