This guide covers all of the requirements covered by the PCI DSS and highlights what part of the WISP addresses each control. If you have any questions, please contact support@blackhatconsultants.com and we will be happy to assist.

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

1.1 Establish firewall and router configuration standards that include the following:
   - WISP CM-06 Configuration Settings

1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations
   - WISP CM-02 Baseline Configurations
   - WISP CM-06 Configuration Settings

1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks
   - WISP CM-08 Information System Component Inventory

1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
   - WISP SC-07 Boundary Protection
   - WISP SC-03 Security Function Isolation

1.1.4 Description of groups, roles, and responsibilities for logical management of network components
   - WISP CM-09 Configuration Management Plan

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. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.
   - WISP CM-07 Least Functionality
1.1.6 Requirement to review firewall and router rule sets at least every six months
   - WISP AC-04 Information Flow Enforcement (Access Control Lists)

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity’s ability to control or manage.
   - WISP SC-02 Application Partitioning

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
   - WISP SC-07 Boundary Protection
   - WISP CM-07 Least Functionality

1.2.2 Secure and synchronize router configuration files.
   - WISP CM-02 Baseline Configurations

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.
   - WISP SC-03 Security Function Isolation

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.
   - WISP SC-03 Security Function Isolation
   - WISP CA-03 Information System Connections

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
   - WISP SC-03 Security Function Isolation
   - WISP CA-03 Information System Connections

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.
   - WISP CA-03 Information System Connections

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.
   - WISP AC-04 Information Flow Enforcement (Access Control Lists)
   - WISP CA-03 Information System Connections

1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.
   - WISP CA-03 Information System Connections

1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
   - WISP AC-04 Information Flow Enforcement (Access Control Lists)
   - WISP CA-03 Information System Connections

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only ?established? connections are allowed into the network.)
   - WISP AC-04 Information Flow Enforcement (Access Control Lists)

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.
   - WISP SC-03 Security Function Isolation
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.
  - WISP SC-03 Security Function Isolation

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.
  - WISP SC-03 Security Function Isolation

**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.
  - WISP IA-05 Authenticator Management (Passwords)

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.
  - WISP IA-05 Authenticator Management (Passwords)

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.
  - WISP PM-07 Enterprise Architecture
  - WISP SA-08 Security Engineering Principles

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.)
  - WISP SC-03 Security Function Isolation

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.
  - WISP CM-07 Least Functionality

2.2.3 Configure system security parameters to prevent misuse.
  - WISP CM-06 Configuration Settings

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
  - WISP CM-07 Least Functionality

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.
  - WISP MA-04 Non-Local Maintenance

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.
  - WISP SA-009 External Information Systems
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.

- WISP SA-12 Information Output Handling & Retention

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.
- WISP SA-12 Information Output Handling & Retention

3.2 Do not store sensitive authentication data after authorization (even if encrypted).

- WISP SA-12 Information Output Handling & Retention

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.

Note: In the normal course
- WISP SA-12 Information Output Handling & Retention

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.
- WISP SA-12 Information Output Handling & Retention

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.
- WISP SA-12 Information Output Handling & Retention

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).
- WISP SA-12 Information Output Handling & Retention

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
- WISP MP-04 Media Storage
- WISP SC-28 Encrypting Data At Rest

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.
- WISP SC-28 Encrypting Data At Rest

3.5 Protect any keys used to secure cardholder data against disclosure and misuse: Note: This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.
- WISP SA-12 Information Output Handling & Retention
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.
   - WISP SA-12 Information Output Handling & Retention

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.
   - WISP SA-12 Information Output Handling & Retention

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:
   - WISP SA-12 Information Output Handling & Retention

3.6.1 Generation of strong cryptographic keys
   - WISP SA-12 Information Output Handling & Retention

3.6.2 Secure cryptographic key distribution
   - WISP SA-12 Information Output Handling & Retention

3.6.3 Secure cryptographic key storage
   - WISP SA-12 Information Output Handling & Retention

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).
   - WISP SA-12 Information Output Handling & Retention

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.
   - WISP SA-12 Information Output Handling & Retention

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).
   - WISP SA-12 Information Output Handling & Retention

3.6.7 Prevention of unauthorized substitution of cryptographic keys.
   - WISP SA-12 Information Output Handling & Retention

3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.
   - WISP SA-12 Information Output Handling & Retention
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.
   - WISP SC-08 Transmission Integrity
   - WISP SC-13 Use of Cryptography

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.
   - WISP AC-18 Wireless Access

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).
   - WISP PL-04 Rules of Behavior (Acceptable Use)

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).
   - WISP SI-03 Malicious Software (Malware) Protection

5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
   - WISP SI-03 Malicious Software (Malware) Protection

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
   - WISP SI-03 Malicious Software (Malware) Protection

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.
   - WISP SI-02 Flaw Remediation

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.
   - WISP RA-03 Risk Assessment
   - WISP RA-04 Risk Assessment Update

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:
   - WISP SA-10 Developer Configuration Management
   - WISP SA-11 Developer Security Testing

6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers
   - WISP SA-11 Developer Security Testing
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.

- WISP SA-11 Developer Security Testing

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

- WISP SA-11 Developer Security Testing
- WISP CM-04 Security Impact Analysis

6.4.1 Separate development/test and production environments

- WISP CM-04 Security Impact Analysis

6.4.2 Separation of duties between development/test and production environments

- WISP CM-04 Security Impact Analysis

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

- WISP CM-04 Security Impact Analysis

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

- WISP CM-04 Security Impact Analysis

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

- WISP SI-02 Flaw Remediation

6.4.5.1 Documentation of impact.

- WISP SI-02 Flaw Remediation

6.4.5.2 Documented change approval by authorized parties.

- WISP SI-02 Flaw Remediation

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

- WISP SI-02 Flaw Remediation

6.4.5.4 Back-out procedures.

- WISP SI-02 Flaw Remediation

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

- WISP SA-10 Developer Configuration Management

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

- WISP SA-10 Developer Configuration Management

6.5.2 Buffer overflow

- WISP SA-10 Developer Configuration Management

6.5.3 Insecure cryptographic storage

- WISP SA-10 Developer Configuration Management
6.5.4 Insecure communications  
- WISP SA-10 Developer Configuration Management

6.5.5 Improper error handling  
- WISP SA-10 Developer Configuration Management

6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).  
- WISP SA-10 Developer Configuration Management

6.5.7 Cross-site scripting (XSS)  
- WISP SA-10 Developer Configuration Management

6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)  
- WISP SA-10 Developer Configuration Management

6.5.9 Cross-site request forgery (CSRF)  
- WISP SA-10 Developer Configuration Management

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  
- WISP SA-11 Developer Security Testing

**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:  
- WISP AC-03 Access Enforcement

7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities  
- WISP AC-03 Access Enforcement

7.1.2 Assignment of privileges is based on individual personnel’s job classification and function  
- WISP AC-03 Access Enforcement

7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.  
- WISP AC-03 Access Enforcement

7.1.4 Implementation of an automated access control system  
- WISP AC-03 Access Enforcement

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:  
- WISP AC-03 Access Enforcement
7.2.1 Coverage of all system components
- WISP AC-03 Access Enforcement

7.2.2 Assignment of privileges to individuals based on job classification and function
- WISP AC-03 Access Enforcement

7.2.3 Default “deny-all” setting
- WISP AC-03 Access Enforcement

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.
- WISP IA-02 Identification & Authentication

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
- WISP IA-02 Identification & Authentication

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.
- WISP IA-02 Identification & Authentication

8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.
- WISP IA-07 Cryptographic Module Authentication

8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:
- WISP AC-02 Account Management
- WISP IA-05 Authenticator Management (Passwords)

8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- WISP AC-02 Account Management

8.5.2 Verify user identity before performing password resets.
- WISP AC-02 Account Management

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.
- WISP AC-02 Account Management

8.5.4 Immediately revoke access for any terminated users.
- WISP AC-02 Account Management

8.5.5 Remove/disable inactive user accounts at least every 90 days.
- WISP AC-02 Account Management
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.
   - WISP AC-02 Account Management

8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.
   - WISP AC-02 Account Management

8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.
   - WISP AC-02 Account Management

8.5.9 Change user passwords at least every 90 days.
   - WISP AC-02 Account Management

8.5.10 Require a minimum password length of at least seven characters.
   - WISP AC-02 Account Management
   - WISP IA-05 Authenticator Management (Passwords)

8.5.11 Use passwords containing both numeric and alphabetic characters.
   - WISP AC-02 Account Management
   - WISP IA-05 Authenticator Management (Passwords)

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.
   - WISP AC-02 Account Management
   - WISP IA-05 Authenticator Management (Passwords)

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.
   - WISP AC-02 Account Management

8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
   - WISP AC-02 Account Management

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.
   - WISP AC-02 Account Management
   - WISP AC-12 Remote Session Termination

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.
   - WISP AC-02 Account Management
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.
   - WISP PE-03 Physical Access Control

9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: “Sensitive areas” refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.
   - WISP PE-03 Physical Access Control

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.
   - WISP PE-04 Access Control for Transmission Medium

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.
   - WISP PE-04 Access Control for Transmission Medium

9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.
   - WISP PE-07 Visitor Control

9.3 Make sure all visitors are handled as follows:
   - WISP PE-07 Visitor Control

9.3.1 Authorized before entering areas where cardholder data is processed or maintained.
   - WISP PE-07 Visitor Control

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.
   - WISP PE-07 Visitor Control

9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.
   - WISP PE-07 Visitor Control

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.
   - WISP PE-08 Access Records

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.
   - WISP MP-04 Media Storage

9.6 Physically secure all media.
   - WISP MP-04 Media Storage
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:
   - WISP MP-04 Media Storage

9.7.1 Classify media so the sensitivity of the data can be determined.
   - WISP MP-04 Media Storage

9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.
   - WISP MP-04 Media Storage

9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).
   - WISP MP-05 Media Transportation

9.9 Maintain strict control over the storage and accessibility of media.
   - WISP MP-04 Media Storage

9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.
   - WISP MP-05 Media Transportation

9.10 Destroy media when it is no longer needed for business or legal reasons as follows:
   - WISP MP-06 Media Sanitization

9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
   - WISP MP-06 Media Sanitization

9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
   - WISP MP-06 Media Sanitization

**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.
   - WISP AU-01 Audit & Accountability Policy & Procedures

10.2 Implement automated audit trails for all system components to reconstruct the following events:
   - WISP AU-02 Auditable Events

10.2.1 All individual accesses to cardholder data
   - WISP AU-02 Auditable Events

10.2.2 All actions taken by any individual with root or administrative privileges
   - WISP AU-02 Auditable Events

10.2.3 Access to all audit trails
   - WISP AU-02 Auditable Events

10.2.4 Invalid logical access attempts
   - WISP AU-02 Auditable Events

10.2.5 Use of identification and authentication mechanisms
   - WISP AU-02 Auditable Events
10.2.6 Initialization of the audit logs
- WISP AU-02 Auditable Events

10.2.7 Creation and deletion of system-level objects
- WISP AU-02 Auditable Events

10.3 Record at least the following audit trail entries for all system components for each event:
- WISP AU-03 Content of Audit Records

10.3.1 User identification
- WISP AU-03 Content of Audit Records

10.3.2 Type of event
- WISP AU-03 Content of Audit Records

10.3.3 Date and time
- WISP AU-03 Content of Audit Records

10.3.4 Success or failure indication
- WISP AU-03 Content of Audit Records

10.3.5 Origination of event
- WISP AU-03 Content of Audit Records

10.3.6 Identity or name of affected data, system component, or resource.
- WISP AU-03 Content of Audit Records

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.
- WISP AU-08 Time Stamps

10.4.1 Critical systems have the correct and consistent time.
- WISP AU-08 Time Stamps

10.4.2 Time data is protected.
- WISP AU-08 Time Stamps

10.4.3 Time settings are received from industry-accepted time sources.
- WISP AU-08 Time Stamps

10.5 Secure audit trails so they cannot be altered.
- WISP AU-09 Protection of Audit Information

10.5.1 Limit viewing of audit trails to those with a job-related need.
- WISP AU-09 Protection of Audit Information

10.5.2 Protect audit trail files from unauthorized modifications.
- WISP AU-09 Protection of Audit Information

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
- WISP AU-09 Protection of Audit Information
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.
   ▪ WISP AU-09 Protection of Audit Information

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).
   ▪ WISP AU-09 Protection of Audit Information

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). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.
   ▪ WISP SI-04 Information System Monitoring

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).
   ▪ WISP SA-12 Information Output Handling & Retention

**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.
   ▪ WISP AC-18 Wireless Access

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).
   ▪ WISP RA-02 Security Categorization

11.2.1 Perform quarterly internal vulnerability scans.
   ▪ WISP RA-05 Vulnerability Scanning

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).
   ▪ WISP RA-05 Vulnerability Scanning

11.2.3 Perform internal and external scans after any significant change.
   ▪ WISP RA-05 Vulnerability Scanning

11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:
   ▪ WISP RA-05 Vulnerability Scanning

11.3.1 Network-layer penetration tests
   ▪ WISP RA-05 Vulnerability Scanning

11.3.2 Application-layer penetration tests
   ▪ WISP RA-05 Vulnerability Scanning

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.
   ▪ WISP SI-04 Information System Monitoring
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.

- WISP SI-07 Software & Information Integrity

**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:

- WISP PM-01 Information Security Program Plan
- WISP PM-08 Critical Infrastructure Plan

12.1.1 Addresses all PCI DSS requirements.

- WISP AT-02 Security Awareness

12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.

- WISP RA-03 Risk Assessment

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

- WISP RA-03 Risk Assessment

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).

- WISP SI-04 Information System Monitoring

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:

- WISP PL-04 Rules of Behavior (Acceptable Use)

12.3.1 Explicit approval by authorized parties

- WISP PL-04 Rules of Behavior (Acceptable Use)

12.3.2 Authentication for use of the technology

- WISP PL-04 Rules of Behavior (Acceptable Use)

12.3.3 A list of all such devices and personnel with access

- WISP PM-05 Information System Inventory

12.3.4 Labeling of devices to determine owner, contact information and purpose

- WISP PM-05 Information System Inventory

12.3.5 Acceptable uses of the technology

- WISP PL-04 Rules of Behavior (Acceptable Use)

12.3.6 Acceptable network locations for the technologies

- WISP PL-04 Rules of Behavior (Acceptable Use)

12.3.7 List of company-approved products

- WISP PM-05 Information System Inventory

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

- WISP AC-17 Remote Access
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
   - WISP AC-17 Remote Access

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.
   - WISP PL-04 Rules of Behavior (Acceptable Use)

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
   - WISP PL-04 Rules of Behavior (Acceptable Use)

12.5 Assign to an individual or team the following information security management responsibilities:
   - WISP PM-01 Information Security Program Plan
   - WISP PM-02 Assigned Information Security Responsibilities
12.5.1 Establish, document, and distribute security policies and procedures.
   - WISP PM-01 Information Security Program Plan
   - WISP PM-02 Assigned Information Security Responsibilities

12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.
   - WISP PM-01 Information Security Program Plan
   - WISP PM-02 Assigned Information Security Responsibilities

12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
   - WISP PM-01 Information Security Program Plan
   - WISP PM-02 Assigned Information Security Responsibilities

12.5.4 Administer user accounts, including additions, deletions, and modifications
   - WISP PM-01 Information Security Program Plan
   - WISP PM-02 Assigned Information Security Responsibilities

12.5.5 Monitor and control all access to data.
   - WISP PM-02 Assigned Information Security Responsibilities

12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
   - WISP AT-02 Security Awareness

12.6.1 Educate personnel upon hire and at least annually.
   - WISP AT-02 Security Awareness
   - WISP AT-03 Security Training

12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.
   - WISP AT-02 Security Awareness
   - WISP AT-04 Security Training Records
   - WISP AT-05 Contacts With Security Groups & Associations
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.)

- **WISP PS-03 Personnel Screening**

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

- **WISP SA-009 External Information Systems**

12.8.1 Maintain a list of service providers.

- **WISP SA-009 External Information Systems**

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.

- **WISP SA-009 External Information Systems**

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

- **WISP SA-009 External Information Systems**

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

- **WISP SA-009 External Information Systems**

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

- **WISP IR-08 Incident Response Plan (IRP)**

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
- Specific incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response

- **WISP IR-08 Incident Response Plan (IRP)**

12.9.2 Test the plan at least annually.

- **WISP IR-08 Incident Response Plan (IRP)**

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

- **WISP IR-08 Incident Response Plan (IRP)**

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

- **WISP IR-08 Incident Response Plan (IRP)**

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

- **WISP IR-08 Incident Response Plan (IRP)**
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

- WISP IR-08 Incident Response Plan (IRP)