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

1.1 Are firewall and router configuration standards established and implemented to include the following:

- 1.1.1 Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?
- 1.1.2 (a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?
- 1.1.2 (b) Is there a process to ensure the diagram is kept current?
- 1.1.3 Is there a current diagram that shows all cardholder data flows across systems and networks?
- 1.1.4 (a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?
- 1.1.5 Are groups, roles, and responsibilities for logical management of network components assigned and documented?
- 1.1.6 Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?
- 1.1.7 Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?

1.2 Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:

- 1.2.1 (a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?
- 1.2.2 Are router configuration files secured from unauthorized access?
- 1.2.3 Are perimeter firewalls installed between all wireless networks and the cardholder data environment?

1.3 Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:

- 1.3.1 Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?
- 1.3.3 Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network?
- 1.3.5 Are only established connections permitted into the network?

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

2.1 (a) Are vendor-supplied defaults always changed before installing a system on the network?

- 2.1.1 For wireless environments connected to the cardholder data environment, are ALL wireless vendor defaults changed at installations?

2.2 (a) Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards?

- 2.2.1 (a) Is only one primary function implemented per server?
- 2.2.2 Are only necessary services, protocols, and daemons enabled as required for the function of the system?
- 2.2.3 Are additional security features documented and implemented for any required services, protocols, or daemons considered to be insecure?

2.3 Is non-console administrative access encrypted using strong cryptography?

Requirement 3: Protect stored cardholder data

3.1 Are data retention and disposal policies, procedures, and processes implemented as follows:

- (a) Is data storage amount and retention time limited to what is required for legal, regulatory, and/or business requirements?
- (b) Are processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, and/or business reasons?
- (c) Are specific retention requirements for cardholder data defined?
- (d) Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?

3.2 (a) For issuers and companies supporting issuing services, is there a documented business justification for the storage of sensitive authentication data?

- (c) For all other entities: Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?
- (d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization, even if encrypted:
    - 3.2.1 Is full track data not stored after authorization?
    - 3.2.2 Is the card verification code or value not stored after authorization?
    - 3.2.3 Is the personal identification number (PIN) or the encrypted PIN block not stored after authorization?

3.3 Is the PAN masked when displayed such that only personnel with a legitimate business need can see more than the first six and last four digits of the PAN?

3.4 Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs) by using one of the following:

- One-way hashes based on strong cryptography,
- Truncation,
- Index tokens and pads,
- Strong cryptography with associated key management processes?

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

4.1 (a) Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks?

- (b) Are only trusted keys and/or certificates accepted?
- (c) Are security protocols implemented to use only secure configurations, and not to support insecure versions or configurations?
- (d) Is the proper encryption strength implemented for the encryption methodology in use?
- (e) Is TLS enabled whenever cardholder data is transmitted or received?

4.2 (a) Are PANs rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (such as email, instant messaging, SMS, or chat)?

- (b) Are policies in place that prohibit the sending of unprotected PANs via end-user messaging technologies?

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

5.1 Is anti-virus software deployed on all systems commonly affected by malicious software?

5.1.1 Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (viruses, Trojans, worms, spyware, adware, rootkits)?

5.2 (a) Are all anti-virus software and definitions kept current?

- (b) Are automatic updates and periodic scans enabled and being performed?
- (c) Are all anti-virus mechanisms generating audit logs, and are the logs retained in accordance with PCI DSS Requirement 10.7?

5.3 Are all anti-virus mechanisms:

- Actively running?
- Unable to be disabled or altered by users?

Requirement 6: Develop and maintain secure systems and applications

6.1 Is there a process to identify security vulnerabilities, including:

- Using reputable outside sources for vulnerability information?
- Assigning a risk ranking to vulnerabilities, including identification of all high-risk and critical vulnerabilities?

6.2 (a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?

- (b) Are critical security patches installed within one month of release?

6.3 (a) Are software development processes based on industry standards and/or best practices?

- (b) Is information security included throughout the software development life cycle?
- (c) Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging)?
- (d) Are development, test, and custom application accounts, user IDs, and passwords removed before applications become active?

6.4 (a) Are development and test environments separate from production environments?

- (b) Is access control in place to enforce separation between development/test environments and the production environment?

6.4.3 Are production data (live PANs) not used for testing or development?

6.4.5 Are change-control procedures documented and include the following:

- Documentation of impact?
- Documented approval by authorized parties?
- Functionality testing to verify the change does not adversely impact security?
- Back-out procedures?

6.5 (a) Do software development processes address common coding vulnerabilities?

- (b) Are developers trained at least annually in up-to-date secure coding techniques?
- (c) Are applications developed based on secure coding guidelines to protect applications from the following vulnerabilities:
    - 6.5.1 Injection flaws, particularly SQL injection?
    - 6.5.2 Buffer overflow vulnerabilities?
    - 6.5.7 Cross-site scripting (XSS) vulnerabilities?
    - 6.5.8 Improper access control (e.g., insecure direct object references, failure to restrict URL access, directory traversal)?
    - 6.5.9 Cross-site request forgery (CSRF)?
    - 6.5.10 Broken authentication and session management?

6.6 Are public-facing web applications protected against known attacks, either by reviewing them at least annually or by installing an automated technical solution (such as a web application firewall)?

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

7.1 Is access to system components and cardholder data limited to only those individuals whose jobs require such access?

7.1.2 Is access to privileged user IDs restricted as follows:

- To the least privileges necessary to perform job responsibilities?
- Assigned only to roles that specifically require privileged access?

7.1.3 Is access assigned based on individual personnel’s job classification and function?

7.2 Is an access control system in place for systems in the cardholder data environment, which restricts access based on a user’s need to know?

Requirement 8: Identify and authenticate access to system components

8.1.1 Are all users assigned a unique ID before allowing them to access system components or cardholder data?

8.1.3 Is access for terminated users immediately deactivated or removed?

8.1.4 Are inactive user accounts either removed or disabled within 90 days?

8.1.5 (a) Are accounts used by vendors for remote access enabled only during the time period needed and disabled when not in use?

- (b) Are vendor remote access accounts monitored while in use?

8.1.6 Are repeated access attempts limited by locking out the user ID after no more than six attempts?

8.1.7 Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until an administrator enables the user ID?

8.2 In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users:

- Something you know (e.g., a password)?
- Something you have (e.g., a token device or smart card)?
- Something you are (e.g., a biometric)?

8.2.3 Are user password parameters configured to require passwords meet the following:

- A minimum password length of at least seven characters?
- Contain both numeric and alphabetic characters?

Requirement 8 (continued): Identify and authenticate access to system components

8.2.4 Are user passwords changed at least every 90 days?
8.2.5 Must an individual submit a new password that is different from any of the last four passwords they have used?
8.2.6 Are passwords set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?
8.3 Is multi-factor authentication used for all non-console access into the cardholder data environment for personnel with administrative access?
8.5 Are group, shared, or generic accounts, passwords, or other authentication methods prohibited?
8.6 Where other authentication mechanisms are used (such as physical or logical security tokens, smart cards, and certificates), is the use of these mechanisms assigned as follows:

- To an individual account?
- Only the intended account can use the mechanism to gain access?

Requirement 9: Restrict physical access to cardholder data

9.1 Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?
9.1.1 Are either video cameras or access-control mechanisms in place to monitor individual physical access to sensitive areas?
9.1.2 (a) Are physical and/or logical controls implemented to restrict access to publicly accessible

network jacks?
9.1.2 (b) Are physical and/or logical controls implemented to restrict physical access to wireless access points, gateways, and handheld devices?
9.2 Are procedures in place to distinguish between onsite personnel and visitors (for example, assigning ID badges)?
9.3 Are visitors identified and restricted to non-sensitive areas or escorted in sensitive areas?
9.4 Are all media physically secured?
9.5 Are storage containers used for materials that contain information to be destroyed (such as hard copy materials) secured to prevent access to the contents?
9.6 (a) Is strict control maintained over the internal or external distribution of any kind of media?

- (b) Are all media classified to determine its sensitivity?
- (c) Is media sent via secured courier or other delivery method that can be accurately tracked?
  9.7 Is strict control maintained over the storage and accessibility of media?
  9.8 Is all media destroyed when it is no longer needed for business or legal reasons?
  9.8.1 Are hardcopy materials containing cardholder data crosscut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?

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

10.1 Are audit trails implemented to link all access to system components to each individual user?
10.2 Are automated audit trails implemented for all system components to reconstruct the following events:

- 10.2.1 All individual user accesses to cardholder data?
- 10.2.2 All actions taken by any individual with root or administrative privileges?
- 10.2.3 Access to all audit trails?
- 10.2.4 Invalid logical access attempts?
- 10.2.5 Use of and changes to identification and authentication mechanisms—including the creation of new accounts and elevation of privileges?
- 10.2.6 Initialization, stopping, or pausing of audit logs?
- 10.2.7 Creation and deletion of system-level objects?

10.3 Are the following audit trail entries recorded for all system components for each event:

- 10.3.1 User identification?
- 10.3.2 Type of event?
- 10.3.3 Date and time?
- 10.3.4 Success or failure indication?
- 10.3.5 Origination of event?
- 10.3.6 Identity or name of affected data, system component, or resource?

10.4 Are all critical system clocks and times synchronized across the cardholder data environment using time synchronization technology?
10.5 (a) Is access to audit trails limited to those with a job-related need?

- (b) Are audit trails protected from unauthorized modifications?
- (c) Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?
  10.6 (a) Are logs and security events for all system components reviewed at least daily?
- (b) Are audit logs retained for at least one year?

Requirement 11: Regularly test security systems and processes

11.1 Are processes implemented for detecting wireless access points and preventing unauthorized wireless access to the cardholder data environment?
11.1.1 (a) Is a quarterly test performed to identify and detect all authorized and unauthorized wireless access points?
11.1.1 (b) Are the results of the wireless access point test documented?
11.1.1 (c) Is the methodology used to test for the presence of wireless access points adequate and does it include the following:

- (i) A wireless analyzer to identify authorized and unauthorized wireless devices?
- (ii) Incident response procedures in the event that unauthorized wireless access points are detected?

11.2 Are internal and external vulnerability scans performed, as follows:
11.2.1 (a) Are quarterly internal vulnerability scans performed?
11.2.1 (b) Does the scan process include rescans as needed until:

- (i) For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS?
- (ii) For internal scans, a passing result is obtained or all high-risk vulnerabilities are resolved?

11.3 Does the penetration-testing methodology include the following:

- 11.3.1 (a) Is external penetration testing performed at least annually and after any significant infrastructure or application changes?
- 11.3.2 (a) Is internal penetration testing performed at least annually and after any significant infrastructure or application changes?
- 11.3.3 (a) Are exploitable vulnerabilities found during penetration testing corrected, and does this include repeated testing until vulnerabilities are corrected?
- 11.3.4 (a) Are segmentation controls and methods tested at least annually to ensure they are operational and effective?

11.4 (a) Are intrusion-detection systems and/or intrusion-prevention systems used to monitor all traffic in the cardholder data environment?

- (b) Are IDS/IPS systems configured to alert personnel of suspected compromises?
- (c) Are all traffic at the perimeter of the cardholder data environment and at critical points in the environment monitored?

11.5 Is a change-detection mechanism (such as file-integrity monitoring) deployed to alert personnel to unauthorized modification of critical system files, configuration files, or content files?

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

12.1 Is a security policy established, published, maintained, and disseminated to all relevant personnel?

- 12.1.1 Is the security policy reviewed at least annually and updated when the environment changes?
- 12.1.2 Are daily operational security procedures consistent with all the requirements in PCI DSS?

12.2 Are formal risk assessments performed at least annually and upon significant changes to the environment?

12.3 Are usage policies for critical technologies (such as remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, etc.) established and documented, and do they require the following:

- 12.3.1 Explicit approval by authorized parties?
- 12.3.2 Authentication for use of the technology?
- 12.3.3 A list of all such devices and personnel with access?
- 12.3.4 Acceptable uses of the technology?

12.4 (a) Is a CISO or equivalent formally assigned the responsibility for information security?
12.5 (a) Are the following information security management responsibilities formally assigned to an individual or team:

- 12.5.1 Establishing, documenting, and distributing security policies and procedures?
- 12.5.2 Monitoring and analyzing security alerts and information?
- 12.5.3 Establishing, documenting, and distributing incident response and escalation procedures?
- 12.5.4 Administering user accounts, including additions, deletions, and modifications?
- 12.5.5 Monitoring and controlling all access to data?

12.6 (a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?
12.8 Are policies and procedures maintained to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data?
12.10 Are incident response procedures in place and include the following:

- 12.10.1 Roles, responsibilities, and communication strategies in the event of a compromise?
- 12.10.2 Specific incident response procedures?
- 12.10.3 Business recovery and continuity procedures?
- 12.10.4 Data backup processes?
- 12.10.5 Legal requirements?