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

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?
1.1.4 (b) Is the current network diagram consistent with the firewall configuration standards?
1.1.6 (a) Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification?
1.1.6 (b) Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?
1.2.1 (a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?
1.2.1 (b) Is all other inbound and outbound traffic specifically denied?
1.3.4 Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network?
1.3.5 Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?
1.3.6 Is stateful inspection, also known as dynamic packet filtering, implemented—that is, only established connections are allowed into the network?
1.3.8 (a) Are methods in place to prevent the disclosure of private IP addresses and routing information to the Internet?
1.3.8 (b) Is any disclosure of private IP addresses and routing information to external entities authorized?

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 (b) Are unnecessary default accounts removed or disabled before installing a system on the network?
2.2 (a) Are configuration standards developed for all system components, and are they consistent with industry-accepted system hardening standards?
2.2 (b) Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?
2.2 (c) Are system configuration standards applied when new systems are configured?
2.2 (d) Do system configuration standards include the following:

- Changing all vendor-supplied defaults and elimination of unnecessary default accounts?
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server?
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system?
- Implementing additional security features for any required services, protocols, or daemons that are considered insecure?
- Configuring system security parameters to prevent misuse?
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?

2.2.1 (a) Is only one primary function implemented per server to prevent functions that require different security levels from co-existing on the same server?

2.2.1 (b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?
2.2.2 (a) Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system?
2.2.2 (b) Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?
2.2.3 Are additional security features documented and implemented for any required services, protocols, or daemons that are considered insecure?
2.2.4 (a) Are system administrators knowledgeable about common security parameter settings for system components?
2.2.4 (b) Are common system security parameter settings included in system configuration standards?
2.2.4 (c) Are security parameter settings set appropriately on system components?
2.2.5 (a) Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?
2.2.5 (b) Are enabled functions documented, and do they support secure configuration?
2.2.5 (c) Is only documented functionality present on system components?
2.3 (a) Is non-console administrative access encrypted using technologies such as SSH, VPN, or SSL/TLS?
2.3 (b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?
2.3 (c) Is administrator access to web-based management interfaces encrypted with strong cryptography?
2.3 (d) For the technology in use, is strong cryptography implemented according to industry best practices and/or vendor recommendations?

Requirement 3: Protect stored cardholder data

3.2 (c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?
3.2 (d) Do all systems adhere to the following regarding non-storage of sensitive authentication data after authorization (even if encrypted):

- 3.2.2 The card verification code or value (CVV) is not stored after authorization?
- 3.2.3 The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?

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

4.1 (a) Are strong cryptography and security protocols (such as SSL/TLS, SSH, IPSEC) used to safeguard sensitive cardholder data during transmission over open, public networks?
4.1 (b) Are only trusted keys and/or certificates accepted?
4.1 (c) Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?
4.1 (d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?
4.1 (e) For SSL/TLS implementations, is SSL/TLS enabled whenever cardholder data is transmitted

or received?
4.2 (b) Are policies in place stating that unprotected PANs are not to be sent 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 (e.g., viruses, Trojans, worms, spyware, adware, rootkits)?
5.1.2 Are periodic evaluations performed to identify evolving malware threats in order to confirm whether systems considered to not be commonly affected by malicious software continue as such?
5.2 (a) Are all anti-virus software and definitions kept current?
5.2 (b) Are automatic updates and periodic scans enabled and being performed?
5.2 (c) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?
5.3 Are all anti-virus mechanisms actively running and 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 that includes 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?
  6.2 (b) Are critical security patches installed within one month of release?
  6.4.5 (a) Are change-control procedures for implementing security patches and software modifications documented and requiring the following:
- Documentation of impact?
- Documented change control approval by authorized parties?
- Functionality testing to verify the change does not adversely impact security?
- Back-out procedures?
  6.4.5.1 Documentation of impact?
  6.4.5.2 Documented approval by authorized parties?
  6.4.5.3 (a) Functionality testing to verify the change does not adversely impact security?
  6.4.5.3 (b) For custom code changes, testing of updates for compliance with PCI DSS Requirement 6.5 before being deployed into production?
  6.4.5.4 Back-out procedures?

6.5 Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities:
6.5.1 Do coding techniques address injection flaws, particularly SQL injection?
6.5.2 Do coding techniques address buffer overflow vulnerabilities?

6.5.7 Do coding techniques address cross-site scripting (XSS) vulnerabilities?
6.5.8 Do coding techniques address improper access control (e.g., insecure direct object references, failure to restrict URL access, directory traversal)?
6.5.9 Do coding techniques address cross-site request forgery (CSRF)?
6.5.10 Do coding techniques address broken authentication and session management?
6.6 Are public-facing web applications protected against known attacks by either reviewing them at least annually or 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 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?

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 any terminated users immediately deactivated or removed?
8.1.5 (a) Are accounts used by vendors to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?
8.1.5 (b) Are vendor remote access accounts monitored when in use?
8.1.6 (a) 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, such as a password or passphrase?
- Something you have, such as a token device or smart card?
- Something you are, such as a biometric?
  8.2.1 (a) Is strong cryptography used to render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components?
  8.2.3 (a) Are user password parameters configured to require passwords/passphrases meet the following:
- A minimum password length of at least seven characters?
- Contain both numeric and alphabetic characters?
  8.2.4 (a) Are user passwords/passphrases changed at least every 90 days?
  8.2.5 (a) Must an individual submit a new password/phrase that is different from any of the last four passwords/phrases he or she has used?
  8.2.6 Are passwords/phrases 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 two-factor authentication incorporated for remote network access originating from outside the network by personnel (including users and administrators) and all third parties (including vendor access for support or maintenance)?
8.5 Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows:

- Generic user IDs and accounts are disabled or removed?
- Shared user IDs for system administration activities and other critical functions do not exist?
- Shared and generic user IDs are not used to administer any system components?

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

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

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?
9.5 Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?
9.6 (a) Is strict control maintained over the internal or external distribution of any kind of media?
9.6 (b) Do controls include the following:

- 9.6.1 Is media classified so the sensitivity of the data can be determined?
- 9.6.2 Is media sent by secured courier or other delivery method that can be accurately tracked?
- 9.6.3 Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?

9.7 Is strict control maintained over the storage and accessibility of media?
9.8 (a) Is all media destroyed when it is no longer needed for business or legal reasons?
9.8.1 (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?
9.8.1 (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?

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

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

- 10.2.2 All actions taken by any individual with root or administrative privileges?
- 10.2.4 Invalid logical access attempts?
- 10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to the creation of new accounts and elevation of privileges, and all changes, additions, or deletions to accounts with root or administrative privileges?

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?

10.5.4 Are logs for external-facing technologies (e.g., wireless, firewalls, DNS, mail) written onto a secure, centralized, internal log server or media?
10.6 Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows:

- 10.6.1 (b) Are the following logs and security events reviewed at least daily, either manually or via log tools: security events, logs of all system components that store, process, or transmit CHD, or that could impact the security of CHD, logs of all critical system components, logs of all servers and system components that perform security functions (e.g., firewalls, IDS/IPS, authentication servers, etc.)?
- 10.6.2 (b) Are logs of all other system components periodically reviewed—either manually or via log tools—based on the organization's policies and risk management strategy?
- 10.6.3 (b) Is follow-up to exceptions and anomalies identified during the review process performed?

10.7 (b) Are audit logs retained for at least one year?
10.7 (c) Are at least the last three months' logs immediately available for analysis?

Requirement 11: Regularly test security systems and processes

11.2.2 (a) Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?
11.2.2 (b) Do external quarterly scan and rescan results satisfy the ASV Program Guide requirements for a passing scan (e.g., no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?
11.2.3 (a) Are internal and external scans, and rescans as needed, performed after any significant change?
11.2.3 (b) Does the scan process include rescans until:

- For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS?
- For internal scans, a passing result is obtained, or all high-risk vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?
  11.3 Does the penetration-testing methodology include the following:
- Based on industry-accepted penetration testing approaches (e.g., NIST SP800-115)?
- Includes coverage for the entire CDE perimeter and critical systems?
- Includes testing from both inside and outside the network?
- Includes testing to validate any segmentation and scope-reduction controls?

11.3.1 (a) Is external penetration testing performed at least annually and after any significant infrastructure or application changes?
11.3.3 Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?
11.3.4 (a) Are penetration testing procedures defined to test all segmentation methods, to confirm they are operational and effective?
11.5 (a) Is a change-detection mechanism (e.g., file-integrity monitoring tools) deployed within the cardholder data environment to detect unauthorized modification of critical system files, configuration files, or content files?
11.5 (b) Is the change-detection mechanism configured to alert personnel to unauthorized modification of critical files and to perform critical file comparisons at least weekly?
11.5.1 Is a process in place to respond to any alerts generated by the change-detection solution?

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?
12.4 Do security policy and procedures clearly define information security responsibilities for all personnel?
12.5 (b) Are information security management responsibilities formally assigned to an individual or team for establishing, documenting, and distributing security incident response and escalation procedures?
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 and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data?
12.8.1 Is a list of service providers maintained?
12.8.2 Is a written agreement maintained that includes an acknowledgment that the service providers are responsible for the security of cardholder data they handle?
12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?
12.8.4 Is a program maintained to monitor service providers’ PCI DSS compliance status at least annually?
12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?
12.10.1 (a) Has an incident response plan been created to be implemented in the event of a system breach?

- (b) Does the plan address roles, responsibilities, communication strategies, incident response procedures, business recovery and continuity, data backup processes, legal requirements, coverage of critical system components, and reference to payment brand procedures?