PCI DSS Question		Response		
		Yes	No	N/A
9.9.3.b	Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?	☑	□	
9.10	Are security policies and operational procedures for restricting physical access to cardholder data: * Documented * In use * Known to all affected parties?	☑	□	

Regularly Monitor and Test Networks

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

PCI DSS Question		Response		
		Yes	No	N/A
10.1.a	Are audit trails enabled and active for system components?	☑	□	
10.1.b	Is access to system components linked to individual users?	☑	□	
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?	☑	□	

PCI DSS Question		Response		
		Yes	No	N/A
10.2.5	Use of and changes to identification and authentication mechanisms–including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges?	☑	☐	
10.2.6	Initialization, stopping, or pausing of the audit logs?	☑	☐	
10.2.7	Creation and deletion of system-level object?	☑	☐	
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 through use of time synchronization technology, and is the technology kept current? Note: One example of time synchronization technology is Network Time Protocol (NTP).	☑	☐	
10.4.1	Are the following processes implemented for critical systems to have the correct and consistent time:			
10.4.1.a	Do only designated central time server(s) receive time signals from external sources, and are time signals from external sources based on International Atomic Time or UTC?	☑	☐	
10.4.1.b	Where there is more than one designated time server, do the time servers peer with each other to keep accurate time?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
10.4.1.c	Do systems receive time only from designated central time server(s)?	☑	☐	
10.4.2	Is time data is protected as follows:			
10.4.2.a	Is access to time data restricted to only personnel with a business need to access time data?	☑	☐	
10.4.2.b	Are changes to time settings on critical systems logged, monitored, and reviewed?	☑	☐	
10.4.3	Are time settings received from specific, industry accepted time sources? (This is to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	☑	☐	
10.5	Are audit trails secured so they cannot be altered, as follows:			
10.5.1	Is viewing of audit trails limited to those with a job-related need?	☑	☐	
10.5.2	Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?	☑	☐	
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	☑	☐	
10.5.4	Are logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) written onto a secure, centralized, internal log server or media?	☑	☐	
10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
10.6	Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows? Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.			
10.6.1.a	Are written policies and procedures defined for reviewing the following at least daily, either manually or via log tools? * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	☑	□	
10.6.1.b	Are the following logs and security events reviewed at least daily, either manually or via log tools? * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	☑	□	
10.6.2.a	Are written policies and procedures defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy?	☑	□	
10.6.2.b	Are reviews of all other system components performed in accordance with organization’s policies and risk management strategy?	☑	□	
10.6.3.a	Are written policies and procedures defined for following up on exceptions and anomalies identified during the review process?	☑	□	
10.6.3.b	Is follow up to exceptions and anomalies performed?	☑	□	

PCI DSS Question		Response		
		Yes	No	N/A
10.7.a	Are audit log retention policies and procedures in place and do they require that logs are retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)?	☑	□	
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?	☑	□	
10.9	Are security policies and operational procedures for monitoring all access to network resources and cardholder data: * Documented * In use * Known to all affected parties?	☑	□	

Requirement 11: Regularly test security systems and processes

PCI DSS Question		Response		
		Yes	No	N/A
11.1.a	Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis? Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.	☑	□	□
11.1.b	Does the methodology detect and identify any unauthorized wireless access points, including at least the following? * WLAN cards inserted into system components; * Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and * Wireless devices attached to a network port or network device.	☑	□	□

PCI DSS Question		Response		
		Yes	No	N/A
11.1.c	If wireless scanning is utilized to identify authorized and unauthorized wireless access points, is the scan performed at least quarterly for all system components and facilities?	☑	□	□
11.1.d	If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?	☑	□	□
11.1.1	Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?	☑	□	□
11.1.2.a	Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?	☑	□	□
11.1.2.b	Is action taken when unauthorized wireless access points are found?	☑	□	□
11.2	Are internal and external network vulnerability scans run 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), as follows: Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.			
11.2.1.a	Are quarterly internal vulnerability scans performed?	☑	□	□
11.2.1.b	Does the quarterly internal scan process address all "high risk" vulnerabilities and include rescans to verify all "high-risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved?	☑	□	□

PCI DSS Question		Response		
		Yes	No	N/A
11.2.1.c	Are quarterly internal scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	☑	□	□
11.2.2.a	Are quarterly external vulnerability scans performed? Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.	☑	□	□
11.2.2.b	Do external quarterly scan and rescan results satisfy the ASV Program Guide requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?	☑	□	□
11.2.2.c	Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?	☑	□	□
11.2.3.a	Are internal and external scans, and rescans as needed, performed after any significant change? Note: Scans must be performed by qualified personnel.	☑	□	□
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?	☑	□	□
11.2.3.c	Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	☑	□	□

PCI DSS Question		Response		
		Yes	No	N/A
11.3	Does the penetration-testing methodology include the following? * Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) * Includes coverage for the entire CDE perimeter and critical systems * Includes testing from both inside and outside the network * Includes testing to validate any segmentation and scope-reduction controls * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 * Defines network-layer penetration tests to include components that support network functions as well as operating systems * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months * Specifies retention of penetration testing results and remediation activities results	☑	□	□
11.3.1.a	Is external penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	☑	□	□
11.3.1.b	Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	☑	□	□
11.3.2.a	Is internal penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	☑	□	□
11.3.2.b	Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	☑	□	□
11.3.3	Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?	☑	□	□
11.3.4	If segmentation is used to isolate the CDE from other networks:			

PCI DSS Question		Response		
		Yes	No	N/A
11.3.4.a	Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?	☑	□	□
11.3.4.b	Does penetration testing to verify segmentation controls meet the following? * Performed at least annually and after any changes to segmentation controls/methods * Covers all segmentation controls/methods in use * Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	☑	□	□
11.3.4.c	Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	☑	□	□
11.4.a	Are intrusion-detection and/or intrusion-prevention techniques that detect and/or prevent intrusions into the network in place to monitor all traffic: * At the perimeter of the cardholder data environment, and * At critical points in the cardholder data environment.	☑	□	□
11.4.b	Are intrusion-detection and/or intrusion-prevention techniques configured to alert personnel of suspected compromises?	☑	□	□
11.4.c	Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?	☑	□	□
11.5.a	Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed within the cardholder data environment to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files? Examples of files that should be monitored include: * System executables * Application executables * Configuration and parameter files * Centrally stored, historical or archived, log, and audit files * Additional critical files determined by entity (for example, through risk assessment or other means)	☑	□	□

PCI DSS Question		Response		
		Yes	No	N/A
11.5.b	Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly? Note: For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).	☑	☐	☐
11.5.1	Is a process in place to respond to any alerts generated by the change-detection solution?	☑	☐	☐
11.6	Are security policies and operational procedures for security monitoring and testing: * Documented * In use * Known to all affected parties?	☑	☐	☐

Maintain an Information Security Policy

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

PCI DSS Question		Response		
		Yes	No	N/A
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?	☑	☐	