| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 3.5 | Are keys used to secure stored cardholder data protected against disclosure and misuse as follows:<br>Note: This requirement applies to keys used to encrypt stored cardholder data, and 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. | | | |
| 3.5.2 | Is access to cryptographic keys restricted to the fewest number of custodians necessary? | ☑ | □ | |
| 3.5.3 | Are secret and private cryptographic keys used to encrypt/decrypt cardholder data stored in one (or more) of the following forms at all times?<br>* Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key<br>* Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)<br>* As at least two full-length key components or key shares, in accordance with an industry-accepted method.<br>Note: It is not required that public keys be stored in one of these forms. | ☑ | □ | |
| 3.5.4 | Are cryptographic keys stored in the fewest possible locations? | ☑ | □ | |
| 3.6.a | Are all key-management processes and procedures fully documented and implemented for cryptographic keys used for encryption of cardholder data? | ☑ | □ | |
| 3.6.c | Are key-management processes and procedures implemented to require the following: | | | |
| 3.6.1 | Do cryptographic key procedures include the generation of strong cryptographic keys? | ☑ | □ | |
| 3.6.2 | Do cryptographic key procedures include secure cryptographic key distribution? | ☑ | □ | |
| 3.6.3 | Do cryptographic key procedures include secure cryptographic key storage? | ☑ | □ | |

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 3.6.4 | Do cryptographic key procedures include cryptographic key changes for keys that have reached the end of their defined 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)? | ☑ | □ | |
| 3.6.5.a | Do cryptographic key procedures include retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key)? | ☑ | □ | |
| 3.6.5.b | Do cryptographic key procedures include replacement of known or suspected compromised keys? | ☑ | □ | |
| 3.6.5.c | If retired or replaced cryptographic keys are retained, are these keys only used for decryption/verification purposes, and not used for encryption operations? | ☑ | □ | |
| 3.6.6 | If manual clear-text key-management operations are used, do cryptographic key procedures include split knowledge and dual control of cryptographic keys as follows:<br>* Do split knowledge procedures require that key components are under the control of at least two people who only have knowledge of their own key components?<br>AND<br>* Do dual control procedures require that at least two people are required to perform any key management operations and no one person has access to the authentication materials (for example, passwords or keys) of another?<br>Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction. | ☑ | □ | |
| 3.6.7 | Do cryptographic key procedures include the prevention of unauthorized substitution of cryptographic keys? | ☑ | □ | |
| 3.6.8 | Are cryptographic key custodians required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities? | ☑ | □ | |

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 3.7 | Are security policies and operational procedures for protecting stored cardholder data:<br>* Documented<br>* In use<br>* Known to all affected parties? | ☑ | ☐ | |

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

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 4.1.a | Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks?<br>Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS). | ☑ | ☐ | |
| 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 TLS implementations, is TLS enabled whenever cardholder data is transmitted or received?<br>For example, for browser-based implementations:<br>* "HTTPS" appears as the browser Universal Record Locator (URL) protocol, and<br>* Cardholder data is only requested if "HTTPS" appears as part of the URL. | ☑ | ☐ | |

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 4.1.1 | Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment? | ☑ | ☐ | |
| 4.2.a | Are PANs rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.)? | ☑ | ☐ | |
| 4.2.b | Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies? | ☑ | ☐ | |
| 4.3 | Are security policies and operational procedures for encrypting transmissions of cardholder data:<br>* Documented<br>* In use<br>* Known to all affected parties? | ☑ | ☐ | |
| Appendix A2 | A2.1<br>For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS:<br>* Are the devices confirmed to not be susceptible to any known exploits for SSL/early TLS, or:<br>* Is there a formal Risk Mitigation and Migration Plan in place per Requirement A2.2?<br>A2.2<br>Is there a formal Risk Mitigation and Migration Plan in place for all implementations that use SSL and/or early TLS (other than as allowed in A2.1), that includes:<br>* Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;<br>* Risk assessment results and risk reduction controls in place;<br>* Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;<br>* Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;<br>* Overview of migration project plan including target migration completion date no later than 30th June 2018? | | | |

# Maintain a Vulnerability Management Program

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

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 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 (for example, viruses, Trojans, worms, spyware, adware, and rootkits)? | ☑ | ☐ | |
| 5.1.2 | Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such? | ☑ | ☐ | |
| 5.2 | Are all anti-virus mechanisms maintained as follows: | | | |
| 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:<br>* Actively running?<br>* Unable to be disabled or altered by users?<br>Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active. | ☑ | ☐ | |
| 5.4 | Are security policies and operational procedures for protecting systems against malware:<br>* Documented<br>* In use<br>* Known to all affected parties? | ☑ | ☐ | |

## Requirement 6: Develop and maintain secure systems and applications

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 6.1 | Is there a process to identify security vulnerabilities, including the following:<br>* Using reputable outside sources for vulnerability information?<br>* Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities?<br>Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.<br>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data. | ☑ | ☐ | |
| 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?<br>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | ☑ | ☐ | |
| 6.3.a | Are software-development processes based on industry standards and/or best practices? | ☑ | ☐ | ☐ |
| 6.3.b | Is information security included throughout the software-development life cycle? | ☑ | ☐ | ☐ |
| 6.3.c | Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging)? | ☑ | ☐ | ☐ |
| 6.3.d | Do software development processes ensure the following at 6.3.1 - 6.3.2: | | | |

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 6.3.1 | Are development, test, and/or custom application accounts, user IDs, and passwords removed before applications become active or are released to customers? | ☑ | □ | □ |
| 6.3.2 | Is all custom code reviewed prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated processes as follows:<br><br>* Are code changes reviewed by individuals other than the originating code author, and by individuals who are knowledgeable about code review techniques and secure coding practices?<br>* Do code reviews ensure code is developed according to secure coding guidelines?<br>* Are appropriate corrections are implemented prior to release?<br>* Are code review results are reviewed and approved by management prior to release?<br><br>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6. | ☑ | □ | □ |
| 6.4 | Are change control processes and procedures followed for all changes to system components to include the following: | | | |
| 6.4.1.a | Are development/test environments separate from the production environment? | ☑ | □ | □ |
| 6.4.1.b | Is access control in place to enforce the separation between the development/test environments and the production environment? | ☑ | □ | □ |
| 6.4.2 | Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment? | ☑ | □ | □ |
| 6.4.3 | Are production data (live PANs) not used for testing or development? | ☑ | □ | □ |
| 6.4.4 | Are test data and accounts removed before production systems become active / goes into production? | ☑ | □ | □ |

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 6.4.5.a | Are change-control procedures documented and require the following?<br>* Documentation of impact<br>* Documented change control approval by authorized parties<br>* Functionality testing to verify that the change does not adversely impact the security of the system<br>* Back-out procedures | ☑ | □ | □ |
| 6.4.5.b | Are the following performed and documented for all changes: | | | |
| 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 that the change does not adversely impact the security of the system? | ☑ | □ | □ |
| 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? | ☑ | □ | □ |
| 6.4.6 | Upon completion of a significant change, are all relevant PCI DSS requirements implemented on all new or changed systems and networks, and documentation updated as applicable? | ☑ | □ | □ |
| 6.5.a | Do software-development processes address common coding vulnerabilities? | ☑ | □ | □ |
| 6.5.b | Are developers trained at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities? | ☑ | □ | □ |

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 6.5.c | Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities:<br>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are update d (for example, the Open Web Application Security Project (OWASP) Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. | | | |
| 6.5.1 | Do coding techniques address injection flaws, particularly SQL injection?<br>Note: Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | ☑ | □ | □ |
| 6.5.2 | Do coding techniques address buffer overflow vulnerabilities? | ☑ | □ | □ |
| 6.5.3 | Do coding techniques address insecure cryptographic storage? | ☑ | □ | □ |
| 6.5.4 | Do coding techniques address insecure communications? | ☑ | □ | □ |
| 6.5.5 | Do coding techniques address improper error handling? | ☑ | □ | □ |
| 6.5.6 | Do coding techniques address all "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)? | ☑ | □ | □ |
| 6.5.7 | Do coding techniques address cross-site scripting (XSS) vulnerabilities? | ☑ | □ | □ |
| 6.5.8 | Do coding techniques address improper access control such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions? | ☑ | □ | □ |
| 6.5.9 | Do coding techniques address cross-site request forgery (CSRF)? | ☑ | □ | □ |
| 6.5.10 | Do coding techniques address broken authentication and session management? | ☑ | □ | □ |

| PCI DSS Question | | Response | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 6.6 | For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying either of the following methods?<br><br>* Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows:<br>* At least annually<br>* After any changes<br>* By an organization that specializes in application security<br>* That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment<br>* That all vulnerabilities are corrected<br>* That the application is re-evaluated after the corrections<br><br>Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.<br><br>– OR–<br><br>* Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) as follows:<br>* Is situated in front of public-facing web applications to detect and prevent web-based attacks.<br>* Is actively running and up to date as applicable.<br>* Is generating audit logs.<br>* Is configured to either block web-based attacks, or generate an alert that is immediately investigated. | ☑ | □ | □ |
| 6.7 | Are security policies and operational procedures for developing and maintaining secure systems and applications:<br><br>* Documented<br>* In use<br>* Known to all affected parties? | ☑ | □ | □ |

# Implement Strong Access Control Measures

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

| PCI DSS Question | Response | | |
|---|---|---|---|
| | Yes | No | N/A |