# Provisions for all PCI DSS V4.0 Requirements

<table>
<thead>
<tr>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Install and Maintain Network Security Controls</strong></td>
</tr>
</tbody>
</table>
| 1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.  
  All security policies and operational procedures that are identified in Requirement 1 are: |
| • Documented.  
  • Kept up to date.  
  • In use.  
  • Known to all affected parties.  
  1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.  
  Information Assurance  
  1.2 Network security controls (NSCs) are configured and maintained.  
  Configuration standards for NSC rulesets are: |
| • Defined.  
  • Implemented.  
  • Maintained.  
  • Change control process defined at Requirement 6.5.1.  
  • An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.  
  • An accurate data flow diagram(s) is maintained that meets the following:  
    • Shows all account data flows across systems and networks.  
    • All security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.  
  • Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.  
  • Applicable configuration rulesets are implemented.  
  • Kept consistent with active network configurations.  
  • Network access to and from the cardholder data environment is restricted.  
  • Known to all affected parties.  
  • In use.  
  • Documented.  
  • Known to all affected parties.  
  • Information Assurance |
| **2 Apply Secure Configurations to All System Components** |
| 2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.  
  All security policies and operational procedures that are identified in Requirement 2 are: |
| • Documented.  
  • Kept up to date.  
  • In use.  
  • Known to all affected parties.  
  2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.  
  Information Assurance  
  2.2 System components are configured and managed securely.  
  Configuration standards are developed, implemented, and maintained to: |
| • Cover all system components.  
  • Address all known security vulnerabilities.  
  • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.  
  • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.  
  • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.  
  • Vendor default accounts are managed as follows:  
    • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.  
    • If the vendor default account(s) will not be used, the account is removed or disabled.  
  Information Assurance  
  Departmental |

Texas Tech University Health Sciences Center El Paso

HSCEP OP: 50.37 Attachment B

August 1, 2023
## Provisions for all PCI DSS V4.0 Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary functions requiring different security levels are managed as follows:</td>
<td>IT CyberSecurity Office / Computer Services</td>
</tr>
<tr>
<td>• Only one primary function exists on a system component, OR</td>
<td>Computer Services</td>
</tr>
<tr>
<td>• Primary functions with differing security levels that exist on the same system component are isolated from each other, OR</td>
<td>IT CyberSecurity Office / Computer Services</td>
</tr>
<tr>
<td>• Primary functions with differing security levels are all secured to the level</td>
<td>IT CyberSecurity Office / Computer Services</td>
</tr>
<tr>
<td>2.2.3 required by the function with the highest security need. Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed</td>
<td>Network Operations</td>
</tr>
<tr>
<td>2.2.4 or disabled. If any insecure services, protocols, or daemons are present:</td>
<td>Network Operations</td>
</tr>
<tr>
<td>• Business justification is documented. Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.</td>
<td>IT CyberSecurity Office / Computer Services</td>
</tr>
<tr>
<td>2.2.5 System security parameters are configured to prevent misuse.</td>
<td>IT CyberSecurity Office / Computer Services</td>
</tr>
<tr>
<td>2.2.7 All non-console administrative access is encrypted using strong cryptography.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>2.3 Wireless environments are configured and managed securely. For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: Default wireless encryption keys. Passwords on wireless access points. SNMP defaults.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>3.1 Processes and mechanisms for protecting stored account data are defined and understood. All security policies and operational procedures that are identified in Requirement 3 are: Documented. Kept up to date. In use. Known to all affected parties.</td>
<td>Accounting Services</td>
</tr>
<tr>
<td>3.1.1 Known to all affected parties.</td>
<td>Accounting Services</td>
</tr>
<tr>
<td>3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.</td>
<td>Accounting Services</td>
</tr>
<tr>
<td>3.2 Storage of account data is kept to a minimum. Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: Coverage for all locations of stored account data. Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. Limiting data storage amount and retention time to that which is required for legal or regulatory, and business requirements. Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. A process for reviewing, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.</td>
<td>Departmental / Accounting Services</td>
</tr>
<tr>
<td>3.3 Sensitive authentication data (SAD) is not stored after authorization. SAD is not released after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.3.1 The full contents of any track are not retained upon completion of the authorization process.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.3.1.1 The full contents of any track are not retained upon completion of the authorization process.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.3.1.2 The card verification code is not retained upon completion of the authorization process.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.3.3 Additional requirement for service providers only</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>3.4 Access to displays of full PAN and ability to copy PAN is restricted. PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.5 Primary account number (PAN) is secured wherever it is stored. PAN is rendered unreadable anywhere it is stored by using any of the following approaches: One-way hashes based on strong cryptography of the entire PAN. Truncation (hashing cannot be used to replace the truncated segment of PAN). If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN.</td>
<td>Departmental</td>
</tr>
<tr>
<td>3.5.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1), are keyed cryptographic hashes of the entire PAN, with associated key management processes and procedures in accordance with Requirements 3.6 and 3.7.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>3.5.1.1 and 3.7. If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: On removable electronic media OR If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets specific requirements.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>3.5.1.2 Requirement 3.5.1. If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render PAN unreadable, it is managed as follows: Logical access is managed separately and independently of native operating system authentication and access control mechanisms.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>• Encryption keys are not associated with user accounts.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>• Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>3.6 Cryptographic keys used to protect stored account data are secured. Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: Access to keys is restricted to the fewest number of custodians necessary. Key-encrypting keys are at least as strong as the data-encrypting keys they protect. Key-encrypting keys are stored separately from data-encrypting keys.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>3.6.1 Keys are stored securely in the fewest possible locations and forms.</td>
<td>IT CyberSecurity Office</td>
</tr>
<tr>
<td>3.6.1.1 Additional requirement for service providers only</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
Provisions for all PCI DSS V4.0 Requirements

### Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times:
- 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.
- Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device.

3.6.1.2 At least two full-length key components or key shares, in accordance with an industry-accepted method.

3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.

3.6.1.4 Cryptographic keys are stored in the fewest possible locations.

Where cryptography is used to protect stored account data, key-management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

3.7 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.

3.7.1 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.

3.7.2 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.

3.7.3 Key-management policies and procedures for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following:
- A defined cryptoperiod for each key type in use.
- A process for key changes at the end of the defined cryptoperiod.
- Key-management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when:
  - The key has reached the end of its defined cryptoperiod.
  - The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known.
- The key is suspected of or known to be compromised.

3.7.4 Retired or replaced keys are not used for encryption operations.

Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.

3.7.6 Key-management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.

3.7.7 Key-management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

3.7.8 Additional requirement for service providers only

Not Applicable

4 Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

4.1 All security policies and operational procedures that are identified in Requirement 4 are:
- Documented.
- Kept up to date.
- In use.

4.1.1 Known to all affected parties.

Information Assurance

4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.

Information Assurance

4.2 PAN is protected with strong cryptography during transmission.

Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:
- Only trusted keys and certificates are accepted.
- Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bulletin is a best practice until its effective date; refer to Applicability Notes below for details.
- The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.

4.2.1 Encryption strength is appropriate for the encryption methodology in use.

Information Assurance

4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.

Information Assurance

Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

4.2.1.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.

Information Assurance

5 Protect All Systems and Networks from Malicious Software

Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

5.1 All security policies and operational procedures that are identified in Requirement 5 are:
- Documented.
- Kept up to date.
- In use.

5.1.1 Known to all affected parties.

Information Assurance

Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.

5.1.2 New requirement - effective immediately

Information Assurance

5.2 Malicious software (malware) is prevented, or detected and addressed.

An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement

5.2.1 The deployed anti-malware solution(s) is kept current via automatic updates.

Information Assurance

5.2.2 Removes, blocks, or contains all known types of malware.

Information Assurance

5.2.3 Confirmation whether such system components continue to not require anti-malware protection.

Information Assurance

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.
# Provisions for all PCI DSS V4.0 Requirements

## Responsibility

### Security vulnerabilities are identified and addressed.

- **5.1.2** Perform periodic scans or active real-time scans.
  - IT CyberSecurity Office

- **5.3.2** Perform continuous behavioral analysis of systems or processes.
  - If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.1.3.
  - IT CyberSecurity Office

- **5.3.2.1** For removable electronic media, the anti-malware solution(s):
  - Performs automatic scans of when the media is inserted, connected, or logically mounted.
  - If removable electronic media is logically mounted.
  - IS CyberSecurity Office

- **5.3.4** Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.
  - IT CyberSecurity Office

- **5.3.5** Management on a case-by-case basis for a limited time period.
  - IT CyberSecurity Office

### Anti-phishing mechanisms protect users against phishing attacks.

- **6.2.3.1** If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:
  - Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.
  - Software Application Support

### Develop and Maintain Secure Systems and Software

#### 6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

- All security policies and operational procedures that are identified in Requirement 6 are:
  - Documented.
  - Kept up to date.
  - In use.

- **6.1.1** Known to all affected parties.
  - Information Assurance

#### 6.2 Bespoke and custom software are developed securely.

- Bespoke and custom software are developed securely, as follows:
  - Based on industry standards and/or best practices for secure development.
  - In accordance with PCI DSS for (example, secure authentication and logging).
  - Incorporating consideration of information security issues during each stage of the software development lifecycle.

- **6.2.1** Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:
  - On software security relevant to their job function and development languages.
  - Including secure software design and secure coding techniques.

- **6.2.2** Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

- Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:
  - Code reviews ensure code is developed according to secure coding guidelines.
  - Code reviews look for both existing and emerging software vulnerabilities.

- **6.2.3** Appropriate corrections are implemented prior to release.

- If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:
  - Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.

#### 6.2.3.1 Reviewed and approved by management prior to release.

- Software Application Support

#### Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:

- Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).
- Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.
- Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

#### 6.2.4 Requirement 6.3.1

- Software Application Support

### Security vulnerabilities are identified and addressed.

- **6.3.1** All security policies and operational procedures that are identified in Requirement 6 are:
  - Documented.
  - Kept up to date.
  - In use.

- **6.3.1** Known to all affected parties.
  - Information Assurance

- **6.3.2** All bespoke and custom software components incorporated into bespoke and custom software are maintained to facilitate vulnerability and patch management.
  - Information Assurance

- **6.3.3** All system components are protected from known vulnerabilities by installing applicable security patches or updates as follows:
  - Critical or high-security patches or updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
  - All other applicable security patches or updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

- **6.4** Public-facing web applications are protected against attacks.
  - IT CyberSecurity Office / Datacenter Operations / Computer Services
# Provisions for all PCI DSS V4.0 Requirements

For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:
  - At least once every 12 months and after significant changes.
  - Including, at a minimum, all common software attacks in Requirement 6.2.4.
  - All vulnerabilities are ranked in accordance with Requirement 6.3.1.
  - All vulnerabilities are corrected.
- The application is re-evaluated after the corrections OR
- Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:
  - Installed in front of public-facing web applications to detect and prevent web-based attacks.
  - Actively running and up to date as applicable.
  - Generating audit logs.

6.4.1 Configured to either block web-based attacks or generate an alert that is immediately investigated.

For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:

- Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.
- Actively running and up to date as applicable.
- Generating audit logs.

6.4.2 Configured to either block web-based attacks or generate an alert that is immediately investigated.

All payment page scripts that are loaded and executed in the consumer’s browser are managed as follows:

- A method is implemented to confirm that each script is authorized.
- A method is implemented to assure the integrity of each script.

6.4.3 An inventory of all scripts is maintained with written justification as to why each is necessary.

6.5 Changes to all system components are managed securely.

Changes to all system components in the production environment are made according to established procedures that include:

- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.

6.5.1 Procedures to address failures and return to a secure state.

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

- Pre-production environments are separated from production environments and the separation is enforced with access controls.

6.5.2 Access controls.

Roles and functions are separated between production and pre-production environments to provide accountability and ensure that only reviewed and approved changes are deployed.

6.5.4 Access to system components and data resources that is based on users’ job classification and functions.

Access is assigned to users, including privileged users, based on:

- The least privileges required (for example, user, administrator) to perform a job function.
- Access to system components and data resources that is based on users’ job classification and functions.
- Appropriate access depending on the entity’s business and access needs.

An access control model is defined and includes granting access as follows:

- Known to all affected parties.
- Documented.
- Kept up to date.
- In use.

7.1 Access to system components and cardholder data by business need to know:

Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood:

- All security policies and operational procedures that are identified in Requirement 7 are:
  - Documented.
  - Kept up to date.
  - In use.

7.1.1 Access to all affected parties.

7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.

An access control model is defined and includes granting access as follows:

- Access is assigned to users, including privileged users, based on:
  - Job classification and function.

7.2.1 Access to system components and data resources that is based on users’ job classification and functions.

Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.

7.2.2 Least privileges necessary to perform job responsibilities.

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.

7.2.4 Management acknowledges that access remains appropriate.

All access control setup is based on least privileges necessary for the operability of the system or application.

7.2.5 Access is limited to the systems, applications, or processes that specifically require their use.

All access by application and system accounts and related access privileges are reviewed as follows:

- Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).
- The application/system access remains appropriate for the function being performed.
- Any inappropriate access is addressed.

7.2.6 Only the responsible administrator(s) can directly access or query repositories of stored CHD.

7.3 Access to system components and data is managed via an access control system(s).

An access control system(s) is in place that restricts access based on a user’s need to know and covers all system components.

- An access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.

7.3.2 Based on job classification and function.

7.3.3 The access control system(s) is set to “deny all” by default.

7.4 Security layers and perimeter protection for system components.

Departmental
Provisions for all PCI DSS V4.0 Requirements

8.1 understood.
     All security policies and operational procedures that are identified in Requirement 8 are:
     - Documented.
     - Kept up to date.
     - In use.

8.1.1 Known to all affected parties.

8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.
User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed. Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:
- Account use is prevented unless needed for an exceptional circumstance.
- Use is limited to the time needed for the exceptional circumstance.
- Business justification for use is documented.
- Use is explicitly approved by management.

8.2.2 Every action taken is attributable to an individual user.

8.2.3 Additional requirement for service providers only
Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:
- Authorized with the appropriate approval.
- Implemented with only the privileges specified on the documented approval.
- Access for terminated users is immediately revoked.
- Inactive user accounts are removed or disabled within 90 days of inactivity.
- Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:
  - Enabled only during the time period needed and disabled when not in use.

8.2.4 Use is monitored for unexpected activity.
If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.

8.3 Strong authentication for users and administrators is established and managed.
All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.

8.3.1 User identity is verified before modifying any authentication factor.
Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.

8.3.2 User identity is verified before modifying any authentication factor.
Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.

8.3.3 User identity is verified before modifying any authentication factor.
Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.

8.3.4 User identity is verified before modifying any authentication factor.
Invalid authentication attempts are limited by:
- Locking out the user ID after not more than 10 attempts.
- Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.
- If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
  - Set to a unique value for first-time use and upon reset.

8.3.5 Forced to be changed immediately after the first use.
If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:
- A minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.
- The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.
MFA is implemented for all non-console access into the CDE for personnel with administrative access.
MFA is implemented for all access into the CDE.
MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows:
- All remote access by all personnel, both users and administrators, originating from outside the entity's network.

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.
MFA systems are implemented as follows:
- The MFA system is not susceptible to replay attacks.
  - MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.
  - At least two different types of authentication factors are used.
- Success
- At least two different types of authentication factors are used.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.
<table>
<thead>
<tr>
<th>#</th>
<th>Provisions for all PCI DSS V4.0 Requirements</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Processes and mechanisms for restricting physical access to cardholder data are defined and understood.</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>9.1.1</td>
<td>All security policies and operational procedures that are identified in Requirement 9 are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Documented.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Kept up to date.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• In use.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Known to all affected parties.</td>
<td></td>
</tr>
<tr>
<td>9.1.2</td>
<td>Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>9.2.1</td>
<td>Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.</td>
<td>Departmental</td>
</tr>
<tr>
<td></td>
<td>• Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Entry and exit points to/from sensitive areas within the CDE are monitored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitoring devices or mechanisms are protected from tampering or disabling.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Collected data is reviewed and correlated with other entries.</td>
<td></td>
</tr>
<tr>
<td>9.2.1.1</td>
<td>Collected data is stored for at least three months, unless otherwise restricted by law.</td>
<td>Departmental / Police Department</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.</td>
<td>Network Operations / Departmental</td>
</tr>
<tr>
<td>9.2.3</td>
<td>Telecommunication lines within the facility is restricted.</td>
<td>Network Operations</td>
</tr>
<tr>
<td>9.2.4</td>
<td>Access to consoles in sensitive areas is restricted via locking when not in use.</td>
<td>IT CyberSecurity Office / Departmental</td>
</tr>
</tbody>
</table>

**Restrict Physical Access to Cardholder Data**

- Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:
  - Identifying personnel.
  - Managing changes to an individual’s physical access requirements.
  - Revoking or terminating personnel identification.
- Limiting access to the identification process or system to authorized personnel.
- Physical access to sensitive areas within the CDE for personnel is controlled as follows:
  - Access is authorized and based on individual job function.
  - Access is revoked immediately upon termination.
- All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.
- Procedures are implemented for authorizing and managing visitor access to the CDE, including:
  - Visitors are authorized before entering.
  - Visitors are escorted at all times.
  - Visitors are clearly identified and given a badge or other identification that expires.
  - Visitor badges or other identification visibly distinguishes visitors from personnel.
  - Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.
  - A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including:
    - The name of the personnel authorizing physical access.
    - The date and time of the visit.
    - The name of the personnel authorizing physical access.
- Media with cardholder data is securely stored, accessed, distributed, and destroyed.
- All media with cardholder data is classified in accordance with the sensitivity of the data.
- Media with cardholder data sent outside the facility is secured as follows:
  - Media sent outside the facility is logged.
  - Materials are stored in secure storage containers prior to destruction.
  - Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons, as follows:
    - The electronic media is destroyed.
  - The cardholder data is rendered unrecoverable so that it cannot be reconstructed.
- Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.
  - POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:
    - Maintaining a list of POI devices.
    - Periodically inspecting POI devices to look for tampering or unauthorized substitution.
    - Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of POI devices.
<table>
<thead>
<tr>
<th>#</th>
<th>Provisions for all PCI DSS V4.0 Requirements</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5.1.1</td>
<td>Device serial number or other methods of unique identification.</td>
<td>Departmental / Accounting Services</td>
</tr>
<tr>
<td>9.5.1.2</td>
<td>POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.</td>
<td>Departmental</td>
</tr>
<tr>
<td>9.5.1.2.1</td>
<td>The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.</td>
<td>Compliance</td>
</tr>
<tr>
<td>10.1</td>
<td>Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>10.1.1</td>
<td>Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>10.2</td>
<td>Audit logs are enabled for all system components and cardholder data.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Audit logs capture all individual user access to cardholder data.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.1</td>
<td>Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.2</td>
<td>Audit logs capture all access to audit logs.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.3</td>
<td>Audit logs capture all invalid logical access attempts.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.4</td>
<td>Audit logs capture all changes to identification and authentication credentials including, but not limited to:</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.5</td>
<td>Creation of new accounts.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.6</td>
<td>Elevation of privileges.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.7</td>
<td>Logs of all system components that store, process, or transmit CHD and/or SAD.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.8</td>
<td>Logs of internal systems.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.9</td>
<td>Logs of external systems.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.2.1.10</td>
<td>Logs of all system components (those not specified in Requirement 10.4.1) are reviewed periodically.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.3</td>
<td>Audit logs are protected from destruction and unauthorized modifications.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Audit log files are limited to those with a business need.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal storage location.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.3.3</td>
<td>File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.4</td>
<td>Audit logs are reviewed to identify anomalies or suspicious activity.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.5</td>
<td>Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>10.6</td>
<td>Time-synchronization mechanisms support consistent time settings across all systems.</td>
<td>I.T. - Data Center</td>
</tr>
<tr>
<td>10.6.1</td>
<td>System clocks and time are synchronized using time-synchronization technology.</td>
<td>I.T. - Data Center</td>
</tr>
<tr>
<td>10.6.1.1</td>
<td>Systems are configured to use accurate and consistent time as follows:</td>
<td>I.T. - Data Center</td>
</tr>
<tr>
<td>10.6.1.2</td>
<td>Time synchronization settings and data are protected as follows:</td>
<td>I.T. - Data Center</td>
</tr>
<tr>
<td>10.6.2</td>
<td>Time is synchronized between systems using a central time server.</td>
<td>I.T. - Data Center</td>
</tr>
<tr>
<td>10.6.3</td>
<td>Access to time data is restricted to only personnel with a business need.</td>
<td>I.T. - Data Center</td>
</tr>
<tr>
<td>10.7.1</td>
<td>Additional requirement for service providers only</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
Provisions for all PCI DSS V4.0 Requirements

Information Assurance

Information Technology

Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.

I.T. Cybersecurity

Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

An inventory of authorized wireless access points is maintained, including a documented business justification.

Network Operations

Information Technology

I.T. Cybersecurity

Responsibility

I.T. Cybersecurity

11 Test Security of Systems and Networks Regularly

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

All security policies and operational procedures that are identified in Requirement 11 are:

- Documented.
- Kept up to date.
- In use.

11.1.1 Known to all affected parties.

Information Technology

I.T. Cybersecurity

11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.

Information Technology

Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

Authorized and unauthorized wireless access points are managed as follows:

- The presence of wireless (Wi-Fi) access points is tested for.
- All authorized and unauthorized wireless access points are detected and identified.
- Testing, detection, and identification occurs at least once every three months.

11.2.1 If automated monitoring is used, personnel are notified via generated alerts.

11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.

Network Operations

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

Internal vulnerability scans are performed as follows:

- At least once every three months.
- High-risk and critical vulnerabilities (per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
- Recans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved.
- The scan tool is kept up to date with latest vulnerability information.

11.3.1 Scans are performed by qualified personnel and organizational independence of the tester exists.

I.T. Cybersecurity

All other applicable vulnerabilities (those not ranked as high-risk or critical (per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:

- Addressed based on the risk defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

11.3.1.1 Recans are conducted as needed.

I.T. Cybersecurity

Internal vulnerability scans are performed via authenticated scanning as follows:

- Systems that are unable to accept credentials for authenticated scanning are documented.
- If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.
- High-risk and critical vulnerabilities (per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
- Recans are conducted as needed.
- Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

11.3.1.2 External vulnerability scans are performed as follows:

- At least once every three months.
- By a PCI SSC Approved Scanning Vendor (ASV).
- Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
- Recans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

11.3.2 External vulnerability scans are performed after any significant change as follows:

- Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
- Recans are conducted as needed.
- Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

11.4 Penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

A penetration testing methodology is defined, documented, and implemented by the entity, and includes:

- Industry-accepted penetration testing approaches.
- Coverage for the entire CDE perimeter and critical systems.
- Testing from both inside and outside the network.
- Testing to validate any segmentation and scope-reduction controls.
- Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4.
- Network-layer penetration tests that encompass all components that support network functions as well as operating systems.
- Review and consideration of threats and vulnerabilities experienced in the last 12 months.
- Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.

11.4.1 Retention of penetration testing results and remediation activities results for at least 12 months.

Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.

Departmental
<table>
<thead>
<tr>
<th>#</th>
<th>Provisions for all PCI DSS V4.0 Requirements</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3.3</td>
<td>Organizational independence of the tester exists (not required to be a QSA or ASV).</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>11.4.3</td>
<td>In accordance with the entity’s assessment of the risk posed by the security issue as defined in Requirement 6.3.1.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>11.4.4</td>
<td>Penetration testing is repeated to verify the corrections.</td>
<td>I.T. Cybersecurity</td>
</tr>
<tr>
<td>11.4.5</td>
<td>Penetration testing is repeated to verify the corrections.</td>
<td>I.T. Cybersecurity</td>
</tr>
</tbody>
</table>

### 11.5 Network Intrusions and Unexpected File Changes Are Detected and Responded To

A change-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows:

- All traffic is monitored at the perimeter of the CDE.
- All traffic is monitored at critical points in the CDE.
- Personnel are alerted to suspected compromises.

A comprehensive information security policy that governs and provides direction for protection of the entity’s information assets is known and current.

An overall information security policy is:

- Established.
- Published.
- Maintained.

The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.

Responsibility for the cardholder data environment is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.

Each PCI DSS requirement that provides flexibility for

Examine documented how frequently it is performed (for example, policies and procedures). requirements to be performed periodically is supported by a targeted risk analysis that is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.

Performance of updated risk analyses when needed, as determined by the annual review.

Performance of updated risk analyses when needed, as determined by the annual review.

InformationAssurance

Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following:

- An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used.
- Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use.

A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.

I.T. Cybersecurity

HSCEP OP 50.37
Attachment B
Page 10 of 12
August 1, 2023
# Provisions for all PCI DSS V4.0 Requirements

**Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:**
- Analysis that the technologies continue to receive security fixes from vendors promptly.
- Analysis that the technologies continue to support (and do not preclude) the entity’s PCI DSS compliance.
- Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced “end of life” plans for a technology.
- Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced “end of life” plans.

**12.3.4 PCI DSS compliance is managed.**

**12.4.1 Additional requirement for service providers only.**

**12.4.2 Additional requirement for service providers only.**

**12.4.2.1 Additional requirement for service providers only.**

**12.5.1 PCI DSS scope is documented and validated.**

**12.5.1.1 Documented and maintained keep current.**

**12.5.1.2 Documented and maintained keep current.**

**12.5.2.1 Additional requirement for service providers only.**

**12.5.3 Additional requirement for service providers only.**

**12.6.1 Policy and procedures, and their role in protecting the cardholder data.**

**12.6.1.1 The security awareness program is:**
- Reviewed at least once every 12 months, and
- Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity’s CDE.

**12.6.2 CDE, or the information provided to personnel about their role in protecting cardholder data.**

**12.6.2.1 Personnel receive security awareness training as follows:**
- Upon hire and at least once every 12 months.
- Multiple methods of communication are used.
- Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.

**12.6.3 Security policy and procedures.**

**12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to:**
- Phishing and related attacks.
- Social engineering.

**12.6.3.2 Requirement 12.2.1.**

**12.7 Personnel are screened to reduce risks from insider threats.**

**12.7.1 Potential personnel who will have access to the CDE are screened:**
- Within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.

**12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.**

**12.8.1 A list of third-party service providers (TPSPs) with which account data is shared or that could affect the security of the CDE:**
- Written agreements with TPSPs are maintained as follows:
  - Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
  - Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they are shared between the TPSP and the entity.

**12.8.2 TPSPs included in scope:**
- Written agreements include acknowledgment from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they are shared between the TPSP and the entity.

**12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.**

**12.8.4 Programs are implemented to monitor TPSPs’ PCI DSS compliance status at least once every 12 months.**

**12.8.5 TPSPs are included in scope:**
- Written agreements include acknowledgment from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they are shared between the TPSP and the entity.

**12.9 Third-party service providers (TPSPs) support their customers’ PCI DSS compliance.**

**12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.**

**12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident.**
- The plan includes, but is not limited to:
  - Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
  - Incident response procedures with specific containment and mitigation activities for different types of incidents.
  - Business recovery and continuity procedures.
  - Data backup processes.
  - Analysis of legal requirements for reporting compromises.
  - Coverage and responses of all critical system components.

**12.10.1.1 Reference or inclusion of incident response procedures from the payment brands.**

**12.10.2 At least once every 12 months, the security incident response plan is:**
- Reviewed and the content is updated as needed.

**12.10.2.1 Tested, including all elements listed in Requirement 12.10.1.**

**12.10.3 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained in their incident response responsibilities.**

**12.10.4 The frequency of periodic training for incident response personnel is defined in the entity’s targeted risk analysis.**

**12.10.4.1 which is performed according to all elements specified in Requirement 12.3.1.**

**Responsibility**

- Departmental
- Information Technology/Departmental
- Accounting Services
- Contracting
- Human resource
- Information Technology/Departmental
# Provisions for all PCI DSS V4.0 Requirements

The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:
- Intrusion-detection and intrusion-prevention systems.
- Network security controls.
- Change-detection mechanisms for critical files.
- The change-and-tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.

12.10.5 Detection of unauthorized wireless access points.

The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.

12.10.6 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include:
- Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable.
- Identifying whether sensitive authentication data is stored with PAN.
- Determining where the account data came from and how it ended up where it was not expected.
- Remediation data leaks or process gaps that resulted in the account data being where it was not expected.

12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected.

## Appendix A: Additional PCI DSS Requirements

### Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers. This Appendix is not used for merchant assessments.

### Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

A2.1 POI terminals using SSL and/or early TLS are not susceptible to known SSL/TLS exploits.

A2.1.1 POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.

A2.1.2 Additional requirement for service providers only. Not Applicable

A2.1.3 Additional requirement for service providers only. Not Applicable

### Appendix A3: Designated Entities Supplemental Validation (DESV)

https://www.pcisecuritystandards.org/