PCI DSS Requirements v4.0.1
Requirements
Requirement 1:
1.1 Processes and mechanisms for installing and maintaining network security controls are defined
1.1.1 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 unde
1.2 Network security controls (NSCs) are configured and maintained.
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordar Requirement 6.5.1. **Applicability Notes** Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it pe
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other net **Applicability Notes** A current network diagram(s) or other technical or topological solution that identifies network connections and d
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment. **Applicability Notes** A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across syst requirement.
1.2.5 All services, protocols and ports allowed are identified, approved, and have a defined business need.
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and co
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effe
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations. **Applicability Notes** Any file or setting used to configure or synchronize NSCs is considered to be a “configuration file.” This includes settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.
1.3 Network access to and from the cardholder data environment is restricted.
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary, • All other traffic is specifically denied.
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.

1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless networ

- All wireless traffic from wireless networks into the CDE is denied by default.
- Only wireless traffic with an authorized business purpose is allowed into the CDE.

1.4 Network connections between trusted and untrusted networks are controlled.

1.4.1 NSCs are implemented between trusted and untrusted networks.

1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to:

- Communications with system components that are authorized to provide publicly accessible services, proto
- Stateful responses to communications initiated by system components in a trusted network.
- All other traffic is denied.

Applicability Notes

The intent of this requirement is to address communication sessions between trusted and untrusted networks, r
This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained

1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering th

1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.

Applicability Notes

This requirement is not intended to apply to storage of account data in volatile memory but does apply where m
example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support t
completion of the related payment card transaction).

1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks a

1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned (including the Internet) and the CDE as follows.

- Specific configuration settings are defined to prevent threats being introduced into the entity's network.
- Security controls are actively running.
- Security controls are not alterable by users of the computing devices unless specifically documented and a limited period.

Applicability Notes

These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by
controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures
which these security controls are not active.
This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be
provide opportunities that malicious individuals may exploit.

Requirement 2: App

2.1 Processes and mechanisms for applying secure configurations to all system components are de

2.1.1 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 unde
New requirement - effective immediately

2.2 System components are configured and managed securely.

2.2.1 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
2.2.2 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. **Applicability Notes** This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operatir application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Man This requirement also applies where a system component is not installed within an entity's environment, for exa and are accessed via a cloud subscription service.
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, **OR** • Primary functions with differing security levels that exist on the same system component are isolated from **OR** • Primary functions with differing security levels on the same system component are all secured to the level
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionalit
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure servic
2.2.6 System security parameters are configured to prevent misuse.
2.2.7 All non-console administrative access is encrypted using strong cryptography. **Applicability Notes** This includes administrative access via browser-based interfaces and application programming interfaces (APIs)
2.3 Wireless environments are configured and managed securely.
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor default secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults, • Any other security-related wireless vendor defaults. **Applicability Notes** This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys a • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge wa • Whenever a key is suspected of or known to be compromised.
Requir
3.1 Processes and mechanisms for protecting stored account data are defined and understood.

3.1.1 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.

3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and unde
New requirement - effective immediately

3.2 Storage of account data is kept to a minimum.

3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policie following:

- Coverage for all locations of stored account data.
- Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bulle Applicability Notes below for details.*
- Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or bu
- Specific retention requirements for stored account data that defines length of retention period and includes
- Processes for secure deletion or rendering account data unrecoverable when no longer needed per the rete
- A process for verifying, at least once every three months, that stored account data exceeding the defined r unrecoverable.

Applicability Notes

Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for work TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a d
The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 Ma Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.

3.3 Sensitive authentication data is not stored after authorization.

3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rer authorization process

Applicability Notes

This requirement does not apply to issuers and companies that support issuing services (where SAD is needed f business justification to store the sensitive authentication data.
Refer to Requirement 3.3.3 for additional requirements specifically for issuers.
Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.

3.3.1.1 The full contents of any track are not retained upon completion of the authorization process.

Applicability Notes

In the normal course of business, the following data elements from the track may need to be retained:

- Cardholder name.
- Primary account number (PAN).
- Expiration date.
- Service code.

To minimize risk, store securely only these data elements as needed for business.

3.3.1.2 The card verification code is not retained upon completion of the authorization process.

Applicability Notes

The card verification code is the three- or four-digit number printed on the front or back of a payment card usec

3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the aut

Applicability Notes

PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the F the completion of the authorization process.

3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptograp
Applicability Notes
Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage co
acquirers). Contact the organizations of interest for any additional criteria.
This requirement applies to all storage of SAD, even if no PAN is present in the environment.
Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of aut
This requirement does not apply to issuers and companies that support issuing services where there is a legitim
Refer to Requirement 3.3.3 for requirements specifically for issuers.
This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

3.3.3 ***Additional requirement for issuers and companies that support issuing services and store ser***
authentication data is:

- Limited to that which is needed for a legitimate issuing business need and is secured.
- Encrypted using strong cryptography.

Applicability Notes
This requirement applies only to issuers and companies that support issuing services and store sensitive auther
Entities that issue payment cards or that perform or support issuing services will often create and control sensit
is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication d
store such data.
PCI DSS requirements are intended for all entities that store, process, or transmit account data, including issuer
that sensitive authentication data may be retained if there is a legitimate reason to do so. Any such data must b
and specific payment brand requirements.
(continued on next page)
The bullet above (for encrypting stored SAD with strong cryptography) is a best practice until 31 March 2025, a
and must be fully considered during a PCI DSS assessment.

3.4 Access to displays of full PAN and ability to copy account data is restricted.

3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displ
business need can see more than the BIN and last four digits of the PAN.
Applicability Notes
This requirement does not supersede stricter requirements in place for displays of cardholder data—for example
(POS) receipts.
This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., ar
protection of PAN when stored, processed, or transmitted.

3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all p
authorization and a legitimate, defined business need.
Applicability Notes
Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings t
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

3.5 PAN is secured wherever it is stored.

3.5.1 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).
- Index tokens.
- Strong cryptography with associated key-management processes and procedures.
- Where hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, ar

place to ensure that the different versions cannot be correlated to reconstruct the original PAN.

Applicability Notes

It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to bot

This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadshe

exception, or troubleshooting logs) must all be protected.

This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and de

3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1), are keyed cryptogra

management processes and procedures in accordance with Requirements 3.6 and 3.7.

Applicability Notes

This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadshe

exception, or troubleshooting logs) must all be protected.

This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and de

This requirement is considered a best practice until 31 March 2025, after which it will be required and must be

3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) i

as follows :
- On removable electronic media

OR
- If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that r

Note: Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-manag

Applicability Notes

While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to p

must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encr

data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic me

Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is consi

Requirement 3.5.1 applies.

Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encr

follows:,
- Logical access is managed separately and independently of native operating system authentication and acc
- Decryption keys are not associated with user accounts.
- Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted da

Applicability Notes

Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management

3.6 Cryptographic keys used to protect stored account data are secured.

3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account da

- 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.
- Keys are stored securely in the fewest possible locations and forms.

Applicability Notes

This requirement applies to keys used to encrypt stored account data and to key-encrypting keys used to protec

The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both

Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys requ

3.6.1.1 ***Additional requirement for service providers only:*** A documented description of the cryptographi

- Details of all algorithms, protocols, and keys used for the protection of stored account data, including key s
- Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a be Notes below for details.*
- Description of the key usage for each key.
- Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cr including type and location of devices, as outlined in Requirement 12.3.4.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

In cloud HSM implementations, responsibility for the cryptographic architecture according to this Requirement w customer.

The bullet above (for including, in the cryptographic architecture, that the use of the same cryptographic keys i until 31 March 2025, after which it will be required as part of Requirement 3.6.1.1 and must be fully considered

3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored
- Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved po
- As at least two full-length key components or key shares, in accordance with an industry-accepted method

Applicability Notes

It is not required that public keys be stored in one of these forms.

Cryptographic keys stored as part of a key management system (KMS) that employs SCDs are acceptable.

A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as one of the following:

- Using an approved random number generator and within an SCD,

OR

- According to ISO 19592 or equivalent industry standard for generation of secret key shares.

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

3.6.1.4 Cryptographic keys are stored in the fewest possible locations.

3.7 Where cryptography is used to protect stored account data, key management processes and pr

3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic

3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographi

3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic ke

3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that h the associated application vendor or key owner, and based on industry best practices and guidelines, including

- A defined cryptoperiod for each key type in use.
- A process for key changes at the end of the defined cryptoperiod.

3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destru
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 ke
the key component was known.
- The key is suspected of or known to be compromised.

Retired or replaced keys are not used for encryption operations.

Applicability Notes

If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for exampl

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

Applicability Notes

This control is applicable for manual key-management operations or where key management is not controlled b
A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys st
generated via one of the following:

- Using an approved random number generator and within a secure cryptographic device (SCD), such as a ha
interaction device,

OR

- According to ISO 19592 or equivalent industry standard for generation of secret key shares.

3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized sub

3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians
they understand and accept their key-custodian responsibilities.

3.7.9 ***Additional requirement for service providers only:*** Where a service provider shares cryptographic k
account data, guidance on secure transmission, storage and updating of such keys is documented and distribut

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

Requirement 4: Protect Card

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during tra

4.1.1 All security policies and operational procedures that are identified in Requirement 4 are:

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

4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and unde
New requirement - effective immediately

4.2 PAN is protected with strong cryptography during transmission.

4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmis
- Only trusted keys and certificates are accepted.
- Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid a

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

implementations.

- The encryption strength is appropriate for the encryption methodology in use.

Applicability Notes

There could be occurrences where an entity receives cardholder data unsolicited via an insecure communicatio
receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of the
measures to prevent the channel from being used for cardholder data.

A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organizat
certificate is verified—for example, via hash or signature—and has not expired. Note that self-signed certificates
by” and “issued to” field is the same are not acceptable.

*The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public n
best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully*

4.2.1.1 An inventory of the entity’s trusted keys and certificates used to protect PAN during transmission is ma

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement

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

Applicability Notes

This requirement also applies if a customer, or other third-party, requests that PAN is sent to them via end-user
There could be occurrences where an entity receives unsolicited cardholder data via an insecure communicatio
sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE an
data and implement measures to prevent the channel from being used for cardholder data.

Requirement 5: Prote

5.1 Processes and mechanisms for protecting all systems and networks from malicious software ar

5.1.1 All security policies and operational procedures that are identified in Requirement 5 are:
- Documented
- Kept up to date
- In use
- Known to all affected parties

5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and unde
New requirement - effective immediately

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

5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components
that concludes the system components are not at risk from malware.

5.2.2 The deployed anti-malware solution(s):
- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the followir

- A documented list of all system components not at risk for malware.
- Identification and evaluation of evolving malware threats for those system components.
- Confirmation whether such system components continue to not require anti-malware protection.

Applicability Notes

System components covered by this requirement are those for which there is no anti-malware solution deployed

5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is def
performed according to all elements specified in Requirement 12.3.1.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

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

5.3.2 The anti-malware solution(s):

- Performs periodic scans and active or real-time scans

OR

- Performs continuous behavioral analysis of systems or processes.

5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined
according to all elements specified in Requirement 12.3.1**.**

Applicability Notes

This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

5.3.3 For removable electronic media, the anti-malware solution(s):

- Performs automatic scans of when the media is inserted, connected, or logically mounted,

OR

- Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or lo

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5

5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and au
limited time period.

Applicability Notes

Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized b
protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measu
during which anti-malware protection is not active.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing atta

Applicability Notes

This requirement applies to the automated mechanism. It is not intended that the systems and services providi
are brought into scope for PCI DSS.

The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS

Meeting this requirement for technical and automated controls to detect and protect personnel against phishing
awareness training. Meeting this requirement does not also meet the requirement for providing personnel with

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

Requirement 6: De

6.1 Processes and mechanisms for developing and maintaining secure systems and software are de

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

6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and unde
New requirement - effective immediately

6.2 Bespoke and custom software is developed securely.

6.2.1 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 l

Applicability Notes

This applies to all software developed for or by the entity for the entity’s own use. This includes both bespoke a
software.

6.2.2 Software development personnel working on bespoke and custom software are trained at least once ever
- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

Applicability Notes:

This requirement for code reviews applies to all bespoke and custom software (both internal and public facing),
Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabili
Requirement 6.4.
Code reviews may be performed using either manual or automated processes, or a combination of both.

6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to ider
follows:
- Code reviews ensure code is developed according to secure coding guidelines.
- Code reviews look for both existing and emerging software vulnerabilities.
- Appropriate corrections are implemented prior to release.

6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production,
- Reviewed by individuals other than the originating code author, and who are knowledgeable about code-re
- Reviewed and approved by management prior to release.

Applicability Notes

Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party pers
An individual that has been formally granted accountability for release control and who is neither the original co
being management.

6.2.4 Software engineering techniques or other methods are defined and in use by software development perso
and related vulnerabilities for 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
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shar
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptograph
of operation.
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities th
and channels, client-side functionality, or other system/application functions and resources. This includes cross-
(CSRF).
- Attacks on access control mechanisms, including attempts to bypass or abuse identification, authenticatior
weaknesses in the implementation of such mechanisms.
- Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in

Applicability Notes

This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke a
software.

6.3 Security vulnerabilities are identified and addressed.

6.3.1 Security vulnerabilities are identified and managed as follows:
- New security vulnerabilities are identified using industry-recognized sources for security vulnerability inforr
computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential ir
- Risk rankings, at a minimum, identify all vulnerabilities considered to be a high-risk or critical to the enviror
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and datab

Applicability Notes

This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3
actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to

6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into be
vulnerability and patch management.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches,
- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6
- All other applicable security patches/updates are installed within an appropriate time frame as determined
the environment as identified according to the risk ranking process at Requirement 6.3.1.

6.4 Public-facing web applications are protected against attacks.

6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and
as follows:

- Reviewing public-facing web applications via manual or automated application vulnerability security assess
- At least once every 12 months and after significant changes.
- By an entity that specializes in application security.
- 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 fo
- 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.
- Configured to either block web-based attacks or generate an alert that is immediately investigated.

Applicability Notes

This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2.

This requirement will be superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 becom

6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects a
following:

- Is installed in front of public-facing web applications and is configured to detect and prevent web-based att
- Actively running and up to date as applicable.
- Generating audit logs.
- Configured to either block web-based attacks or generate an alert that is immediately investigated.

Applicability Notes

This new requirement will replace Requirement 6.4.1 once its effective date is reached.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follow

- A method is implemented to confirm that each script is authorized.
- A method is implemented to assure the integrity of each script.
- An inventory of all scripts is maintained with written justification as to why each is necessary.

Applicability Notes

This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fo

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

6.5 Changes to all system components are managed securely.

6.5.1 Changes to all system components in the production environment are made according to established pro

- 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 be
- Procedures to address failures and return to a secure state.

6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place
documentation is updated as applicable.

Applicability Notes

These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmati

6.5.3 Pre-production environments are separated from production environments and the separation is enforced

6.5.4 Roles and functions are separated between production and pre-production environments to provide accou
are deployed.

Applicability Notes

In environments with limited personnel where individuals perform multiple roles or functions, this same goal ca
provide accountability. For example, a developer may also be an administrator that uses an administrator-level
environment and, for their developer role, they use a separate account with user-level access to the production

6.5.5 Live PANs are not used in pre-production environments, except where those environments are included i
applicable PCI DSS requirements.

6.5.6 Test data and test accounts are removed from system components before the system goes into productio

Requirement 7: Restrict Access to S

7.1 Processes and mechanisms for restricting access to system components and cardholder data b

7.1.1 All security policies and operational procedures that are identified in Requirement 7 are:
- Documented,
- Kept up to date
- In use
- Known to all affected parties.

7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and unde
New requirement - effective immediately

7. 2 Access to system components and data is appropriately defined and assigned.

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

7.2.2 Access is assigned to users, including privileged users, based on:
- Job classification and function.
- Least privileges necessary to perform job responsibilities.

7.2.3 Required privileges are approved by authorized personnel.

7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as fo
- At least once every six months
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Applicability Notes

This requirement applies to all user accounts and related access privileges, including those used by personnel a
third-party cloud services.

See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

7.2.5 All application and system accounts and related access privileges are assigned and managed as follows:
- Based on the least privileges necessary for the operability of the system or application.
- Access is limited to the systems, applications, or processes that specifically require their use.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

7.2.5.1 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
- The application/ system access remains appropriate for the function being performed.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

7.2.6 All user access to query repositories of stored cardholder data is restricted as follows:

- Via applications or other programmatic methods, with access and allowed actions based on user roles and
- Only the responsible administrator(s) can directly access or query repositories of stored CHD.

Applicability Notes

This requirement applies to controls for user access to query repositories of stored cardholder data.
See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.

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

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

7.3.2 The access control system(s) is configured to enforce privileges assigned to individuals, applications, and

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

Requirement 8: Identify

8. 1 Processes and mechanisms for identifying users and authenticating access to system compone

8.1.1 All security policies and operational procedures that are identified in Requirement 8 are:

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

8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and unde
New requirement - effective immediately

8.2 User identification and related accounts for users and administrators are strictly managed thro

8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.

Applicability Notes

This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to on
transaction (such as IDs used by cashiers on point-of-sale terminals).

8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when neces

- 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.
- Individual user identity is confirmed before access to an account is granted.
- Every action taken is attributable to an individual user.

Applicability Notes

This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to on
transaction (such as IDs used by cashiers on point-of-sale terminals).

8.2.3 ***Additional requirement for service providers only:*** Service providers with remote access to custom
customer premises.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

This requirement is not intended to apply to service providers accessing their own shared services environment

If service provider employees use shared authentication factors to remotely access customer premises, these fa
accordance with Requirement 8.2.2.

8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are ma

- Authorized with the appropriate approval.
- Implemented with only the privileges specified on the documented approval.

Applicability Notes

This requirement applies to all user accounts, including employees, contractors, consultants, temporary worker

8.2.5 Access for terminated users is immediately revoked

8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.

8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are

- Enabled only during the time period needed and disabled when not in use.
- Use is monitored for unexpected activity.

8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-acti

Applicability Notes

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only o
transaction (such as IDs used by cashiers on point-of-sale terminals).

This requirement is not meant to prevent legitimate activities from being performed while the console/PC is una

8.3 Strong authentication for users and administrators is established and managed.

8.3.1 All user access to system components for users and administrators is authenticated via at least one of the

- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.
- Something you are, such as a biometric element.

Applicability Notes

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only o
transaction (such as IDs used by cashiers on point-of-sale terminals).

This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-sco

A digital certificate is a valid option for “something you have” if it is unique for a particular user.

8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and stora

8.3.3 User identity is verified before modifying any authentication factor.

8.3.4 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.

Applicability Notes

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only o
transaction (such as IDs used by cashiers on point-of-sale terminals).

8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and

- Set to a unique value for first-time use and upon reset.
- Forced to be changed immediately after the first use.

8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the fo

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of
- Contain both numeric and alphabetic characters.

Applicability Notes

This requirement is not intended to apply to:

- User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a point-of-sale terminals).
- Application or system accounts, which are governed by requirements in section 8.6.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.

8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four

Applicability Notes

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only o transaction (such as IDs used by cashiers on point-of-sale terminals).

8.3.8 Authentication policies and procedures are documented and communicated to all users including:

- Guidance on selecting strong authentication factors.
- Guidance for how users should protect their authentication factors.
- Instructions not to reuse previously used passwords/passphrases.
- Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/pas incident.

8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-fac

- Passwords/passphrases are changed at least once every 90 days,

OR

- The security posture of accounts is dynamically analyzed, and real-time access to resources is automatical

Applicability Notes

This requirement applies to in-scope system components that are not in the CDE because these components ar

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only o transaction (such as IDs used by cashiers on point-of-sale terminals).

This requirement does not apply to service providers' customer accounts but does apply to accounts for service

8.3.10 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to custome

- Guidance for customers to change their user passwords/passphrases periodically.
- Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

This requirement does not apply to accounts of consumer users accessing their own payment card information.

This requirement for service providers will be superseded by Requirement 8.3.10.1 once 8.3.10.1 becomes effe

8.3.10.1 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the on any single-factor authentication implementation) then either:

- Passwords/passphrases are changed at least once every 90 days,

OR

- The security posture of accounts is dynamically analyzed, and real-time access to resources is automatical

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

This requirement does not apply to accounts of consumer users accessing their own payment card information.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or

8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are

- Factors are assigned to an individual user and not shared among multiple users.
- Physical and/or logical controls ensure only the intended user can use that factor to gain access.

8.4 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

Applicability Notes

The requirement for MFA for non-console administrative access applies to all personnel with elevated or increas
connection—that is, via logical access occurring over a network interface rather than via a direct, physical conn
MFA is considered a best practice for non-console administrative access to in-scope system components that ar

8.4.2 MFA is implemented for all access into the CDE.

Applicability Notes

This requirement does not apply to:

- Application or system accounts performing automated functions.
- User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a
point-of-sale terminals).

MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to
another instance of MFA to the other type of access. If an individual first connects to the entity's network via re
the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once
network and once when connecting via non-console administrative access from the entity's network into the CD
(continued on next page)

The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-prem
workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as
MFA for remote access into the CDE can be implemented at the network or system/application level; it does not
used when a user connects to the CDE network, it does not have to be used when the user logs into each syste

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that coul

- All remote access by all personnel, both users and administrators, originating from outside the entity's net
- All remote access by third parties and vendors.

Applicability Notes

The requirement for MFA for remote access originating from outside the entity's network applies to all user acc
remote access leads to or could lead to access into the CDE.

If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote
access to that part of the network is not required. However, MFA is required for any remote access to networks
remote access to the entity's networks.

The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-prem
workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.5.1 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 document
basis, for a limited time period.
- At least two different types of authentication factors are used.
- Success of all authentication factors is required before access is granted.

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

8.6 Use of application and system accounts and associated authentication factors are strictly mana

8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follow
- Interactive use is prevented unless needed for an exceptional circumstance.
- Interactive use is limited to the time needed for the exceptional circumstance.
- Business justification for interactive use is documented.
- Interactive use is explicitly approved by management.
- Individual user identity is confirmed before access to account is granted.
- Every action taken is attributable to an individual user.

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are
or bespoke and custom source code. Note: stored passwords/ passphrases are required to be encrypted in acco

Applicability Notes
Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2.
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:
- Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk ana
specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise.
- Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity

Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

Requirement

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and u

9.1.1 All security policies and operational procedures that are identified in Requirement 9 are:
- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and unde
New requirement - effective immediately

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.

9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or p
- Entry and exit points to/from sensitive areas within the CDE are monitored.
- Monitoring devices or mechanisms are protected from tampering or disabling.
- Collected data is reviewed and correlated with other entries.
- Collected data is stored for at least three months, unless otherwise restricted by law.

9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks withi

9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecomm

9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.

9.3 Physical access for personnel and visitors is authorized and managed.

9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, inclu

- 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.

9.3.1.1 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 terminatio

9.3.2 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.

9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the d

9.3.4 A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive

- The visitor’s name and the organization represented.
- The date and time of the visit.
- The name of the personnel authorizing physical access.
- Retaining the log for at least three months, unless otherwise restricted by law.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.4.1 All media with cardholder data is physically secured.

9.4.1.1 Offline media backups with cardholder data are stored in a secure location.

9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once ever

9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.

9.4.3 Media with cardholder data sent outside the facility is secured as follows:

- Media sent outside the facility is logged.
- Media is sent by secured courier or other delivery method that can be accurately tracked.
- Offsite tracking logs include details about media location.

9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when r

Applicability Notes

Individuals approving media movements should have the appropriate level of management authority to grant th such individuals have “manager” as part of their title.

9.4.5 Inventory logs of all electronic media with cardholder data are maintained.

9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.

9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reas

- Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
- Materials are stored in secure storage containers prior to destruction.

Applicability Notes

These requirements for media destruction when that media is no longer needed for business or legal reasons ar which is for securely deleting cardholder data when no longer needed per the entity’s cardholder data retention

9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons v
- The electronic media is destroyed.
- The cardholder data is rendered unrecoverable so that it cannot be reconstructed.

Applicability Notes

These requirements for media destruction when that media is no longer needed for business or legal reasons ar which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention

9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form fa 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

Applicability Notes

These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card fo dipped). This requirement is not intended to apply to manual PAN key-entry components such as computer keyb

This requirement is recommended, but not required, for manual PAN key-entry components such as computer k

This requirement does not apply to commercial off-the-shelf (COTS) devices (for example, smartphones or table for mass-market distribution.

9.5.1.1 An up-to-date list of POI devices is maintained, including:
- Make and model of the device.
- Location of device.
- Device serial number or other methods of unique identification.

9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.

9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in according to all elements specified in Requirement 12.3.1.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacem
- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before gra
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behavior around devices.
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel

Requirement 10: Log and Mo

10.1 Processes and mechanisms for logging and monitoring all access to system components and c

10.1.1 All security policies and operational procedures that are identified in Requirement 10 are:
- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and ur

New requirement - effective immediately

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and

10.2.1 Audit logs are enabled and active for all system components and cardholder data.

10.2.1.1 Audit logs capture all individual user access to cardholder data.

10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interac

10.2.1.3 Audit logs capture all access to audit logs.

10.2.1.4 Audit logs capture all invalid logical access attempts.

10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limite

- Creation of new accounts.
- Elevation of privileges.
- All changes, additions, or deletions to accounts with administrative access.

10.2.1.6 Audit logs capture the following:

- All initialization of new audit logs, and
- All starting, stopping, or pausing of the existing audit logs.

10.2.1.7 Audit logs capture all creation and deletion of system-level objects.

10.2.2 Audit logs record the following details for each auditable event:

- User identification.
- Type of event.
- Date and time.
- Success and failure indication.
- Origination of event.
- Identity or name of affected data, system component, resource, or service (for example, name and protoco

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.3.1 Read access to audit logs files is limited to those with a job-related need.

10.3.2 Audit log files are protected to prevent modifications by individuals.

10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, cer
to modify.

10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing lo

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.4.1 The following audit logs are reviewed at least once daily:

- 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, network security
prevention systems (IDS/IPS), authentication servers).

10.4.1.1 Automated mechanisms are used to perform audit log reviews.
Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodica
Applicability Notes
This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.

10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10
which is performed according to all elements specified in Requirement 12.3.1.
Applicability Notes
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

10.4.3 Exceptions and anomalies identified during the review process are addressed.

10.5 Audit log history is retained and available for analysis.

10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.6.1 System clocks and time are synchronized using time-synchronization technology.

Applicability Notes

Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology

10.6.2 Systems are configured to the correct and consistent time as follows:

- One or more designated time servers are in use.
- Only the designated central time server(s) receives time from external sources.
- Time received from external sources is based on International Atomic Time or Coordinated Universal Time
- The designated time server(s) accept time updates only from specific industry-accepted external sources.
- Where there is more than one designated time server, the time servers peer with one another to keep accu
- Internal systems receive time information only from designated central time server(s).

10.6.3 Time synchronization settings and data are protected as follows:

- Access to time data is restricted to only personnel with a business need.
- Any changes to time settings on critical systems are logged, monitored, and reviewed.

10.7 Failures of critical security control systems are detected, reported, and responded to promptl

10.7.1 ***Additional requirement for service providers only:*** Failures of critical security control systems are but not limited to failure of the following critical security control systems:

- Network security controls
- IDS/IPS
- FIM
- Anti-malware solutions
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

This requirement will be superseded by Requirement 10.7.2 as of 31 March 2025.

10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but control systems:

- Network security controls.
- IDS/IPS.
- Change-detection mechanisms.
- Anti-malware solutions.
- Physical access controls.
- Logical access controls.
- Audit logging mechanisms.
- Segmentation controls (if used).
- Audit log review mechanisms.
- Automated security testing tools (if used).

Applicability Notes

This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as o security control systems not in Requirement 10.7.1.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to:

- Restoring security functions.
- Identifying and documenting the duration (date and time from start to end) of the security failure.
- Identifying and documenting the cause(s) of failure, and documenting required remediation.
- Identifying and addressing any security issues that arose during the failure.
- Determining whether further actions are required as a result of the security failure.
- Implementing controls to prevent the cause of failure from reoccurring.
- Resuming monitoring of security controls.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider, until the 31 March 2025, aft

This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best p which it will be required and must be fully considered during a PCI DSS assessment.

Requirement 11:

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

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

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

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

New requirement - effective immediately

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points

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

Applicability Notes

The requirement applies even when a policy exists that prohibits the use of wireless technology since attackers
Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthoriz
devices that themselves are authorized.

11.2 2 An inventory of authorized wireless access points is maintained, including a documented business justifi

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

11.3.1 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.
- Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been res
- Scan tool is kept up to date with latest vulnerability information.
- Scans are performed by qualified personnel and organizational independence of the tester exists.

Applicability Notes

It is not required to use a QSA or ASV to conduct internal vulnerability scans.

Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the network administrator should not be responsible for scanning the network), or an entity may choose to have int in vulnerability scanning.

11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical (per the entity's vulnerabil
managed as follows:

- Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to
- Rescans are conducted as needed.

Applicability Notes

The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requireme
assets being protected, threats, and likelihood and/or impact of a threat being realized.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows:

- Systems that are unable to accept credentials for authenticated scanning are documented.
- Sufficient privileges are used, for those systems that accept credentials for scanning.
- If accounts used for authenticated scanning can be used for interactive login, they are managed in accorda

Applicability Notes

The authenticated scanning tools can be either host-based or network-based.

"Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducte

This requirement does not apply to system components that cannot accept credentials for scanning. Examples
include some network and security appliances, mainframes, and containers.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

11.3.1.3 Internal vulnerability scans are performed after any significant change as follows:

- High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.
- Rescans are conducted as needed.
- Scans are performed by qualified personnel and organizational independence of the tester exists (not requ

Applicability Notes

Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed afte

11.3.2 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.
- Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* r

Applicability Notes

For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the as
passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every thre
have been corrected as shown in a re-scan(s).

(continued on next page)

However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months

ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target enviro
providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the A

Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan prepa

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

- Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
- Rescans are conducted as needed.
- Scans are performed by qualified personnel and organizational independence of the tester exists (not requ

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabiliti

11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and include

- 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
- Network-layer penetration tests that encompass all components that support network functions as well as o
- 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 securit
- Retention of penetration testing results and remediation activities results for at least 12 months.

Applicability Notes

Testing from inside the network (or “internal penetration testing”) means testing from both inside the CDE and networks.

Testing from outside the network (or “external” penetration testing” means testing the exposed external perim to or accessible to public network infrastructures.

11.4.2 Internal penetration testing is performed:

- Per the entity’s defined methodology
- At least once every 12 months
- After any significant infrastructure or application upgrade or change
- By a qualified internal resource or qualified external third-party
- Organizational independence of the tester exists (not required to be a QSA or ASV).

11.4.3 External penetration testing is performed:

- Per the entity’s defined methodology
- At least once every 12 months
- After any significant infrastructure or application upgrade or change
- By a qualified internal resource or qualified external third party
- Organizational independence of the tester exists (not required to be a QSA or ASV).

11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as fo

- In accordance with the entity’s assessment of the risk posed by the security issue as defined in Require me
- Penetration testing is repeated to verify the corrections.

11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segr

- At least once every 12 months and after any changes to segmentation controls/methods
- Covering all segmentation controls/methods in use.
- According to the entity’s defined penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requ
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

11.4.6 ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from segmentation controls as follows:

- At least once every six months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- According to the entity’s defined penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requ
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

11.4.7 ***Additional requirement for third-party hosted/cloud service providers only:*** Third-party hosted external penetration testing per Requirement 11.4.3 and 11.4.4.

Applicability Notes

To meet this requirement, third-party hosted/cloud service providers may either:

- Provide evidence to its customers to show that penetration testing has been performed according to Requir infrastructure, or
- Provide prompt access to each of their customers, so customers can perform their own penetration testing.

Evidence provided to customers can include redacted penetration testing results but needs to include sufficient 11.4.3 and 11.4.4 have been met on the customer’s behalf.

This requirement applies only when the entity being assessed is a service provider managing third-party hosted

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

11.5 Network intrusions and unexpected file changes are detected and responded to.

11.5.1 Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions

- 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.
- All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.

11.5.1.1 ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-preventi covert malware communication channels.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:

- To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files
- To perform critical file comparisons at least once weekly.

Applicability Notes

For change-detection purposes, critical files are usually those that do not regularly change, but the modification compromise. Change-detection mechanisms such as file integrity monitoring products usually come pre-configu Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, t

11.6 Unauthorized changes on payment pages are detected and responded to.

11.6.1 A change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, ar payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP header and payment page.
- The mechanism functions are performed as follows:

- At least once every seven days

OR

- Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all

Applicability Notes

The intention of this requirement is not that an entity installs software in the systems or browsers of its consum those described under Examples in the PCI DSS Guidance to prevent and detect unexpected script activities.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

Requirement 12: Support inf

12.1 A comprehensive information security policy that governs and provides direction for protectio

12.1.1 An overall information security policy is:

- Established.
- Published.
- Maintained.
- Disseminated to all relevant personnel, as well as to relevant vendors and business partners.

12.1.2 The information security policy is:

- Reviewed at least once every 12 months.
- Updated as needed to reflect changes to business objectives or risks to the environment.

12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and a information security responsibilities.

12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or othe executive management.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including:

- Explicit approval by authorized parties.
- Acceptable uses of the technology.
- List of products approved by the company for employee use, including hardware and software.

Applicability Notes

Examples of end-user technologies for which acceptable use policies are expected, include but are not limited t tablets, mobile phones, and removable electronic media, email usage, and Internet usage.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requi
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 p
realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are s
- Performance of updated risk analyses when needed, as determined by the annual review.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the custo

- Documented evidence detailing each element specified in Appendix B: Guidance and Instructions for Using
controls matrix and risk analysis).
- Approval of documented evidence by senior management.
- Performance of the targeted analysis of risk at least once every 12 months.

New requirement - effective immediately

Applicability Notes

This   only applies to entities using a Customized Approach.

12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 r

- An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and wher
- Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and pro
- A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.

Applicability Notes

The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at lea

- 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 h
- Documentation of a plan, approved by senior management, to remediate outdated technologies, including
plans.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.4 PCI DSS compliance is managed.

12.4.1 ***Additional requirement for service providers only:*** Responsibility is established by executive man
DSS compliance program to include:

- Overall accountability for maintaining PCI DSS compliance.
- Defining a charter for a PCI DSS compliance program and communication to executive management.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

Executive management may include C-level positions, board of directors, or equivalent. The specific titles will d

Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units

12.4.2 ***Additional requirement for service providers only:*** Reviews are performed at least once every thre
tasks in accordance with all security policies and all operational procedures. Reviews are performed by personn
task and include, but not limited to, the following tasks:

- Daily log reviews.
- Configuration reviews for network security controls.
- Applying configuration standards to new systems.
- Responding to security alerts.
- Change-management processes.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

12.4.2.1 Additional requirement for service providers only: Reviews conducted in accordance with Requ

- Results of the reviews.
- Documented remediation actions taken for any tasks that were found to not be performed at Requirement
- Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

12.5 PCI DSS scope is documented and validated.

12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon sign
minimum, the scoping validation includes:

- Identifying all data flows for the various payment stages (for example, authorization, capture settlement, c
example, card-present, card-not-present, and e-commerce).
- Updating all data-flow diagrams per Requirement 1.2.4.
- Identifying all locations where account data is stored, processed, and transmitted, including but not limited
CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.
- Identifying all system components in the CDE, connected to the CDE, or that could impact security of the C
- Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, inclu
- Identifying all connections from third-party entities with access to the CDE.
- Confirming that all identified data flows, account data, system components, segmentation controls, and co
included in scope.

New requirement - effective immediately

Applicability Notes

This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessme
by, the scoping confirmation performed by the entity's assessor during the annual assessment.

12.5.2.1 ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed
significant changes. At a minimum, the scoping validation includes all the elements specified in Requirement 12

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.5.3 ***Additional requirement for service providers only:*** Significant changes to organizational structure
to PCI DSS scope and applicability of controls, with results communicated to executive management.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.6 Security awareness education is an ongoing activity

12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's inform
protecting the cardholder data.

12.6.2 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 enti

their role in protecting cardholder data.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.6.3 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 informatio

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the se
- Phishing and related attacks.
- Social engineering.

Applicability Notes

See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and requirement for providing users security awareness training about phishing and social engineering. These are t met by implementing controls required by the other one.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

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, p sources.

Applicability Notes

For those potential personnel to be hired for positions such as store cashiers, who only have access to one card requirement is a recommendation only.

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

12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect th description for each of the services provided.

Applicability Notes

The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity'

12.8.2 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 th
- Written agreements include acknowledgements from TPSPs that they are responsible for the security of ac

process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's C

Applicability Notes

The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of assigned to each party. The acknowledgment does not have to include the exact wording provided in this requi Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) same as a written agreement specified in this requirement.

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

12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.

Applicability Notes

Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for ex the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable also "not in place" for the entity.

12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are ma
the TPSP and the entity.

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

12.9.1 *Additional requirement for service providers only:* TPSPs acknowledge in writing to customers tha
the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent tha

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of
assigned to each party. The acknowledgment does not have to include the exact wording provided in this requi

12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for inf
providing the following upon customer request:

- PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requiren
- Information about which PCI DSS requirements are the responsibility of the TPSP and which are the respons
responsibilities (Requirement 12.8.5).

New requirement - effective immediately

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to imm

12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed

- Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed
brands and acquirers, at a minimum.
- Incident response procedures with specific containment and mitigation activities for different types of incid
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- 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.
- Tested, including all elements listed in Requirement 12.10.1.

12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed

12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately
responsibilities.

12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted
elements specified in Requirement 12.3.1.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

12.10.5 The security incident response plan includes monitoring and responding to alerts from security monito

- 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 effe*
- Detection of unauthorized wireless access points.

Applicability Notes

The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS ass

12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorp

12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere i

- Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or
- 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.
- Remediating data leaks or process gaps that resulted in the account data being where it was not expected.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

Appendix A1: Addition

A1.1 Multi-tenant service providers protect and segregate all customer environments and data.

A1.1.1 Logical separation is implemented as follows:

- The provider cannot access its customers’ environments without authorization.
- Customers cannot access the provider’s environment without authorization.

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder da

A1.1.3 Controls are implemented such that each customer can only access resources allocated to them.

A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed a

Applicability Notes

The testing of adequate separation between customers in a multi-tenant service provider environment is in add 11.4.6.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.

A1.2.1 Audit log capability is enabled for each customer’s environment that is consistent with PCI DSS Requirer

- Logs are enabled for common third-party applications.
- Logs are active by default.
- Logs are available for review only by the owning customer.
- Log locations are clearly communicated to the owning customer.
- Log data and availability is consistent with PCI DSS Requirement 10

A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in for any customer.

A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed securit

- Customers can securely report security incidents and vulnerabilities to the provider.
- The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities accor

Applicability Notes

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully conside

Appendix A2: Additional PCI DSS Requirements

Note: *SSL/early TLS may not be used as a security control, except by POS POI terminals t*

A2.1.1 Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the known exploits for those protocols.

Applicability Notes

This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requiren the termination or connection point to those POS POI terminals. Requirements A2.1.2 and A2.1.3 apply to POS P The allowance for POS POI terminals that are not currently susceptible to exploits is based on currently known r terminals are susceptible, the POS POI terminals will need to be updated immediately.

A2.1.2 ***Additional requirement for service providers only:*** All service providers with existing connection p as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes:

- Description of usage, including what data is being transmitted, types and number of systems that use and/
- Risk-assessment results and risk-reduction controls in place.
- Description of processes to monitor for new vulnerabilities associated with SSL/early TLS.
- Description of change control processes that are implemented to ensure SSL/early TLS is not implemented
- Overview of migration project plan to replace SSL/early TLS at a future date.

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

A2.1.3 Additional requirement for service providers only: All service providers provide a secure service c

Applicability Notes

This requirement applies only when the entity being assessed is a service provider.

Responsibility			
[3rd Party Vendor]	City of Vancouver	Shared	NA
trols			

nponents

re defined and implemented.

ring Transmission

nd understood.

s Software

oftware

y Business Need to Know

od.

Components

ata

d Cardholder Data

gularly

cies and programs			
urrent.			

ng Providers

resent POS POI Terminal Connections *wn exploits and the termination points to which they connect, as defined in this*			