YourIT!
Your Logo Goes Here

PCI DSS - SAQ D Merchant

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

Purpose

The intended audience for this SAQ includes merchants that handle cardholder data but do not qualify for other SAQ types. This SAQ should be utilized when merchants have complex environments or additional requirements that necessitate a comprehensive assessment. Unique validation requirements include the need for a thorough review of all applicable PCI DSS requirements, with a focus on ensuring compliance across all relevant systems and processes. This SAQ serves as a self-assessment tool to demonstrate compliance with PCI DSS standards.

Scope

This Self-Assessment Questionnaire (SAQ) D for Merchants encompasses all system components, personnel, and processes involved in the storage, processing, or transmission of cardholder data (CHD) within the cardholder data environment (CDE). It includes e-commerce merchants, those with electronic storage of account data, and merchants that do not meet the criteria for other SAQ types. Segmentation must be considered to limit the scope of the assessment, ensuring that all applicable PCI DSS requirements are addressed. This SAQ differs from others by covering a broader range of environments that may have additional PCI DSS requirements.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Requirement 1 - Install and Maintain Network Security Controls

PCI DSS - SAQ D Merchant	Other Requirements
Requirement 1 Install and Maintain Network Security Controls	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.
1.2 Network security controls (NSCs) are configured and maintained.
1.3 Network access to and from the cardholder data environment is restricted.
1.4 Network connections between trusted and untrusted networks are controlled.
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Guidance
Overview
Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.

NSCs examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Typically, NSCs are placed between environments with different security needs or levels of trust, however in some environments NSCs control the traffic to individual devices irrespective of trust boundaries. Policy enforcement generally occurs at layer 3 of the OSI model, but data present in higher layers is also frequently used to determine policy decisions.

Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

NSCs are used to control traffic within an entity's own networks for example, between highly sensitive and less sensitive areas and also to protect the entity's resources from exposure to untrusted networks. The cardholder data environment (CDE) is an example of a more sensitive area within an entity's network. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into sensitive systems. NSCs provide a key protection mechanism for any computer network.

Common examples of untrusted networks include the Internet, dedicated connections such as business-to-business communication channels, wireless networks, carrier networks (such as cellular), third-party networks, and other sources outside the entity's ability to control. Furthermore, untrusted networks also include corporate networks that are considered out-of-scope for PCI DSS, because they are not assessed, and therefore must be treated as untrusted because the existence of security controls has not been verified. While an entity may consider an internal network to be trusted from an infrastructure perspective, if a network is out of scope for PCI DSS, that network must be considered untrusted for PCI DSS.

Refer to Appendix G for definitions of PCI DSS terms.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- PCI-1.1.1 - Requirement 1.1.1:
  Processes and mechanisms for installing and maintaining network security controls are defined and understood.

  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.

  Procedure
  - Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.

- PCI-1.1.2 - Requirement 1.1.2:
  Processes and mechanisms for installing and maintaining network security controls are defined and understood.

  1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.

  Procedure
  - Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned.
  - Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.

- PCI-1.2.1 - Requirement 1.2.1:
  Network security controls (NSCs) are configured and maintained.

  1.2.1 Configuration standards for NSC rulesets are:
  • Defined.
  • Implemented.
  • Maintained.

  Procedure
  - Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement.
  - Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.

- PCI-1.2.2-v4.0.1 - Requirement 1.2.2:
  Network security controls (NSCs) are configured and maintained.

  1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.

Procedure
- Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.
- Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.
- Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.

- PCI-1.2.3 - Requirement 1.2.3:
  Network security controls (NSCs) are configured and maintained.

  1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.

  Procedure
  - Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement.
  - Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.

- PCI-1.2.4 - Requirement 1.2.4:
  Network security controls (NSCs) are configured and maintained.

  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.

  Procedure
  - Examine data-flow diagram(s) and interview personnel to verify the diagram(s) show all account data flows in accordance with all elements specified in this requirement.
  - Examine documentation and interview responsible personnel to verify that the data-flow diagram(s) is accurate and updated when there are changes to the environment.

- PCI-1.2.5 - Requirement 1.2.5:
  Network security controls (NSCs) are configured and maintained.

  1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.

  Procedure
  - Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.
  - Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.

- PCI-1.2.6 - Requirement 1.2.6:
  Network security controls (NSCs) are configured and maintained.

  1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.

Procedure
- Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk.
- Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.

- PCI-1.2.7 - Requirement 1.2.7:
  Network security controls (NSCs) are configured and maintained.

  1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.

  Procedure
  - Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.
  - Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.
  - Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.

- PCI-1.2.8 - Requirement 1.2.8:
  Network security controls (NSCs) are configured and maintained.

  1.2.8 Configuration files for NSCs are:
  • Secured from unauthorized access.
  • Kept consistent with active network configurations.

  Procedure
  - Examine configuration files for NSCs to verify they are in accordance with all elements specified in this requirement.

- PCI-1.3.1 - Requirement 1.3.1:
  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.

  Procedure
  - Examine configuration standards for NSCs to verify that they define restricting inbound traffic to the CDE is in accordance with all elements specified in this requirement.
  - Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.

- PCI-1.3.2 - Requirement 1.3.2:
  Network access to and from the cardholder data environment is restricted.

  1.3.2 Outbound traffic from the CDE is restricted as follows:
  • To only traffic that is necessary.
  • All other traffic is specifically denied.

  Procedure
  - Examine configuration standards for NSCs to verify that they define restricting outbound traffic from the CDE in accordance with all elements specified in this requirement.

- Examine configurations of NSCs to verify that outbound traffic from the CDE is restricted in accordance with all elements specified in this requirement.

- PCI-1.3.3 - Requirement 1.3.3:
  Network access to and from the cardholder data environment is restricted.

  1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:
  • 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.

  Procedure
  - Examine configuration settings and network diagrams to verify that NSCs are implemented between all wireless networks and the CDE, in accordance with all elements specified in this requirement.

- PCI-1.4.1 - Requirement 1.4.1:
  Network connections between trusted and untrusted networks are controlled.

  1.4.1 NSCs are implemented between trusted and untrusted networks.

  Procedure
  - Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.
  - Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.

- PCI-1.4.2 - Requirement 1.4.2:
  Network connections between trusted and untrusted networks are controlled.

  1.4.2 Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.

  Procedure
  - Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.

- PCI-1.4.3 - Requirement 1.4.3:
  Network connections between trusted and untrusted networks are controlled.

  1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.

  Procedure
  - Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.

- PCI-1.4.4 - Requirement 1.4.4:
  Network connections between trusted and untrusted networks are controlled.

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

Procedure
- Examine the data-flow diagram and network diagram to verify that it is documented that system components storing cardholder data are not directly accessible from the untrusted networks.
- Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks.

- PCI-1.4.5 - Requirement 1.4.5:
  Network connections between trusted and untrusted networks are controlled.

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

  Procedure
  - Examine configurations of NSCs to verify that the disclosure of internal IP addresses and routing information is limited to only authorized parties.
  - Interview personnel and examine documentation to verify that controls are implemented such that any disclosure of internal IP addresses and routing information is limited to only authorized parties.

- PCI-1.5.1 - Requirement 1.5.1:
  Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

  1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (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 authorized by management on a case-by-case basis for a limited period.

  Procedure
  - Examine policies and configuration standards and interview personnel to verify security controls for computing devices that connect to both untrusted networks, and the CDE, are implemented in accordance with all elements specified in this requirement.
  - Examine configuration settings on computing devices that connect to both untrusted networks and the CDE to verify settings are implemented in accordance with all elements specified in this requirement.

References
- PCI Security Standards Council Document Library - https://www.pcisecuritystandards.org/document_library/
- PCI Security Standards Council - https://www.pcisecuritystandards.org/
- PCI DSS v4.0 At a Glance - https://www.pcisecuritystandards.org/document_library?category=pcidss&document=dss4aag
- PCI DSS Requirements & Testing Procedure - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Requirement 2 - Apply Secure Configurations to All System Components

PCI DSS - SAQ D Merchant	Other Requirements
Requirement 2 Apply Secure Configurations to All System Components	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.
2.2 System components are configured and managed securely.
2.3 Wireless environments are configured and managed securely.

Guidance
Overview
Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

Refer to Appendix G for definitions of PCI DSS terms.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- PCI-2.1.1 - Requirement 2.1.1:
  Processes and mechanisms for applying secure configurations to all system components are defined and understood.

  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.

  Procedure
  - Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 2 are managed in accordance with all elements specified in this requirement.

- PCI-2.1.2 - Requirement 2.1.2:
  Processes and mechanisms for applying secure configurations to all system components are defined and understood.

2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.

Procedure
- Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 2 are documented and assigned.
- Interview personnel with responsibility for performing activities in Requirement 2 to verify that roles and responsibilities are assigned as documented and are understood.

- PCI-2.2.1 - Requirement 2.2.1:
  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 component is connected to a production environment.

  Procedure
  - Examine system configuration standards to verify they define processes that include all elements specified in this requirement.
  - Examine policies and procedures and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.3.1
  - Examine configuration settings and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.

- PCI-2.2.2 - Requirement 2.2.2:
  System components are configured and managed securely.

  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.

  Procedure
  - Examine system configuration standards to verify they include managing vendor default accounts in accordance with all elements specified in this requirement.
  - Examine vendor documentation and observe a system administrator logging on using vendor default accounts to verify accounts are implemented in accordance with all elements specified in this requirement.
  - Examine configuration files and interview personnel to verify that all vendor default accounts that will not be used are removed or disabled.

- PCI-2.2.3 - Requirement 2.2.3:
  System components are configured and managed securely.

  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 each other,
OR
• Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.

Procedure
- Examine system configuration standards to verify they include managing primary functions requiring different security levels as specified in this requirement.
- Examine system configurations to verify that primary functions requiring different security levels are managed per one of the ways specified in this requirement.
- Where virtualization technologies are used, examine the system configurations to verify that system functions requiring different security levels are managed in one of the following ways: • Functions with differing security needs do not co-exist on the same system component. • Functions with differing security needs that exist on the same system component are isolated from each other. • Functions with differing security needs on the same system component are all secured to the level required by the function with the highest security need.

- PCI-2.2.4 - Requirement 2.2.4:
  System components are configured and managed securely.

  2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.

  Procedure
  - Examine system configuration standards to verify necessary system services, protocols, and daemons are identified and documented.
  - Examine system configurations to verify the following: • All unnecessary functionality is removed or disabled. • Only required functionality, as documented in the configuration standards, is enabled

- PCI-2.2.5 - Requirement 2.2.5:
  System components are configured and managed securely.

  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 services, protocols, or daemons.

  Procedure
  - If any insecure services, protocols, or daemons are present, examine system configuration standards and interview personnel to verify they are managed and implemented in accordance with all elements specified in this requirement.
  - If any insecure services, protocols, or daemons, are present, examine configuration settings to verify that additional security features are implemented to reduce the risk of using insecure services, daemons, and protocols.

- PCI-2.2.6 - Requirement 2.2.6:
  System components are configured and managed securely.

  2.2.6 System security parameters are configured to prevent misuse.

  Procedure

- Examine system configuration standards to verify they include configuring system security parameters to prevent misuse.
- Interview system administrators and/or security managers to verify they have knowledge of common security parameter settings for system components.
- Examine system configurations to verify that common security parameters are set appropriately and in accordance with the system configuration standards.

- PCI-2.2.7 - Requirement 2.2.7:
  System components are configured and managed securely.

  2.2.7 All non-console administrative access is encrypted using strong cryptography.

  Procedure
  - Examine system configuration standards to verify they include encrypting all non-console administrative access using strong cryptography.
  - Observe an administrator log on to system components and examine system configurations to verify that non-console administrative access is managed in accordance with this requirement.
  - Examine settings for system components and authentication services to verify that insecure remote login services are not available for non-console administrative access.

- PCI-2.3.1 - Requirement 2.3.1:
  Wireless environments are configured and managed securely.

  2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:
  • Default wireless encryption keys.
  • Passwords on wireless access points.
  • SNMP defaults.
  • Any other security-related wireless vendor defaults.

  Procedure
  - Examine policies and procedures and interview responsible personnel to verify that processes are defined for wireless vendor defaults to either change them upon installation or to confirm them to be secure in accordance with all elements of this requirement.
  - Examine vendor documentation and observe a system administrator logging into wireless devices to verify: • SNMP defaults are not used. • Default passwords/passphrases on wireless access points are not used.
  - Examine vendor documentation and wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.

- PCI-2.3.2 - Requirement 2.3.2:
  Wireless environments are configured and managed securely.

  2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:
  • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.
  • Whenever a key is suspected of or known to be compromised.

  Procedure

- Interview responsible personnel and examine key-management documentation to verify that wireless encryption keys are changed in accordance with all elements specified in this requirement.

References

- PCI Security Standards Council Document Library - https://www.pcisecuritystandards.org/document_library/
- PCI Security Standards Council - https://www.pcisecuritystandards.org/
- PCI DSS v4.0 At a Glance - https://www.pcisecuritystandards.org/document_library?category=pcidss&document=dss4aag
- PCI DSS Requirements & Testing Procedure - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Requirement 3 - Protect Stored Account Data

PCI DSS - SAQ D Merchant	Other Requirements
Requirement 3 Protect Stored Account Data	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

3.1 Processes and mechanisms for protecting stored account data are defined and understood.
3.2 Storage of account data is kept to a minimum.
3.3 Sensitive authentication data (SAD) is not stored after authorization.
3.4 Access to displays of full PAN and ability to copy PAN are restricted.
3.5 Primary account number (PAN) is secured wherever it is stored.
3.6 Cryptographic keys used to protect stored account data are secured.
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

Note:
Control 3.3.3 is an additional requirement for issuers and companies that support issuing services and store sensitive authentication data.
Controls 3.6.1.1 and 3.7.9 are additional requirements for service providers.

Guidance
Overview
Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk-mitigation opportunities. For example, methods for minimizing risk include not storing account data unless necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies such as e-mail and instant messaging.

If account data is present in non-persistent memory (for example, RAM, volatile memory), encryption of PAN is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. Data should be removed from volatile memory once the business purpose (for example, the associated transaction) is complete. In the case that data storage becomes persistent, all applicable PCI DSS Requirements will apply including encryption of stored data.

Requirement 3 applies to protection of stored account data unless specifically called out in an individual requirement.

Refer to Appendix G for definitions of strong cryptography and other PCI DSS terms.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- PCI-3.1.1 - Requirement 3.1.1:
  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.

Procedure
- Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 3 are managed in accordance with all elements specified in this requirement.

- PCI-3.1.2 - Requirement 3.1.2:
  Processes and mechanisms for protecting stored account data are defined and understood.

  3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.

  Procedure
  - Examine documentation to verify that descriptions of roles and responsibilities performing activities in Requirement 3 are documented and assigned.
  - Interview personnel with responsibility for performing activities in Requirement 3 to verify that roles and responsibilities are assigned as documented and are understood.

- PCI-3.2.1 - Requirement 3.2.1:
  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 policies, procedures, and processes that include at least the following:
  • Coverage for all locations of stored account data.
  • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
  • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
  • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
  • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
  • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

  Procedure
  - Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement.
  - Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy.
  - Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.

- PCI-3.3.1.1-v4.0.1 - Requirement 3.3.1.1:
  Sensitive authentication data (SAD) is not stored after authorization.

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

Procedure
- Examine data sources to verify that the full contents of any track are not stored upon completion of the authorization process.

- PCI-3.3.1.2-v4.0.1 - Requirement 3.3.1.2:
  Sensitive authentication data (SAD) is not stored after authorization.

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

  Procedure
  - Examine data sources, to verify that the card verification code is not stored upon completion of the authorization process.

- PCI-3.3.1.3-v4.0.1 - Requirement 3.3.1.3:
  Sensitive authentication data (SAD) is not stored after authorization.

  3.3.1.3 The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process.

  Procedure
  - Examine data sources, to verify that PINs and PIN blocks are not stored upon completion of the authorization process.

- PCI-3.3.1-v4.0.1 - Requirement 3.3.1:
  Sensitive authentication data (SAD) is not stored after authorization.

  3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.

  Procedure
  - If SAD is received, examine documented policies, procedures, and system configurations to verify the data is not retained after authorization.
  - If SAD is received, examine the documented procedures and observe the secure data deletion processes to verify the data is rendered unrecoverable upon completion of the authorization process.

- PCI-3.3.2-v4.0.1 - Requirement 3.3.2:
  Sensitive authentication data (SAD) is not stored after authorization.

  3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.

  Procedure
  - Examine data stores, system configurations, and/or vendor documentation to verify that all SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.

- PCI-3.3.3-v4.0.1 - Requirement 3.3.3:
  Sensitive authentication data (SAD) is not stored after authorization.

  3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:

Any storage of sensitive authentication data is:
• Limited to that which is needed for a legitimate issuing business need and is secured.
• Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.

Procedure
- Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data: Examine documented policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.
- Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data: Examine data stores and system configurations to verify that the sensitive authentication data is stored securely.

- PCI-3.4.1 - Requirement 3.4.1:
  Access to displays of full PAN and ability to copy PAN is restricted.

  3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.

  Procedure
  - Examine documented policies and procedures for masking the display of PANs to verify: • A list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN is masked when displayed such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.
  - Examine system configurations to verify that full PAN is only displayed for roles with a documented business need, and that PAN is masked for all other requests.
  - Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displayed, and that only those with a legitimate business need are able to see more than the BIN and/or last four digits of the PAN.

- PCI-3.4.2-v4.0.1 - Requirement 3.4.2:
  Access to displays of full PAN and ability to copy PAN is restricted.

  3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.

  Procedure
  - Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.
  - Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.
  - Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote access technologies.

- PCI-3.5.1.1-v4.0.1 - Requirement 3.5.1.1:
  Primary account number (PAN) is secured wherever it is stored.

  3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.

  Procedure
  - Examine documentation about the hashing method used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (as applicable) to verify that the hashing method results in keyed cryptographic hashes of the entire PAN, with associated key management processes and procedures.
  - Examine documentation about the key management procedures and processes associated with the keyed cryptographic hashes to verify keys are managed in accordance with Requirements 3.6 and 3.7
  - Examine data repositories to verify the PAN is rendered unreadable.

- PCI-3.5.1.2-v4.0.1 - Requirement 3.5.1.2:
  Primary account number (PAN) is secured wherever it is stored.

  3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:
  • On removable electronic media
  OR
  • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.

  Procedure
  - Examine encryption processes to verify that, if disk-level or partition-level encryption is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media, OR • If used for non-removable electronic media, examine encryption processes used to verify that PAN is also rendered unreadable via another method that meets Requirement 3.5.1.
  - Examine configurations and/or vendor documentation and observe encryption processes to verify the system is configured according to vendor documentation; the result is that the disk or the partition is rendered unreadable.

- PCI-3.5.1.3 - Requirement 3.5.1.3:
  Primary account number (PAN) is secured wherever it is stored.

  3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render PAN unreadable, it is managed as follows:
  • Logical access is managed separately and independently of native operating system authentication and access control mechanisms.
  • Decryption keys are not associated with user accounts.
  • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.

  Procedure
  - If disk-level or partition-level encryption is used to render PAN unreadable, examine the system configuration and observe the authentication process to verify that logical access is implemented in accordance with all elements specified in this requirement.
  - Examine files containing authentication factors (passwords, passphrases, or cryptographic keys) and interview personnel to verify that authentication factors that allow

access to unencrypted data are stored securely and are independent from the native operating system's authentication and access control methods.

- PCI-3.5.1-v4.0.1 - Requirement 3.5.1:
  Primary account number (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).
  – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN.
  • Index tokens.
  • Strong cryptography with associated key management processes and procedures.

  Procedure
  - Examine documentation about the system used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the methods specified in this requirement.
  - Examine data repositories and audit logs, including payment application logs, to verify the PAN is rendered unreadable using any of the methods specified in this requirement.
  - If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.

- PCI-3.6.1 - Requirement 3.6.1:
  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 data against disclosure and misuse that include:
  • Access to keys is restricted to the fewest number of custodians necessary.
  • Key-encrypting keys are at least as strong as the data-encrypting keys they protect.
  • Key-encrypting keys are stored separately from data-encrypting keys.
  • Keys are stored securely in the fewest possible locations and forms.

  Procedure
  - Examine documented key-management policies and procedures to verify that processes to protect cryptographic keys used to protect stored account data against disclosure and misuse are defined to include all elements specified in this requirement.

- PCI-3.6.1.1 - Requirement 3.6.1.1:
  Cryptographic keys used to protect stored account data are secured.

  3.6.1.1 Additional requirement for service providers only:
  A documented description of the cryptographic architecture is maintained that includes:
  • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date.
  • Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability 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 cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.

Procedure
- Interview responsible personnel and examine documentation to verify that a document exists to describe the cryptographic architecture that includes all elements specified in this requirement.

- PCI-3.6.1.2 - Requirement 3.6.1.2:
  Cryptographic keys used to protect stored account data are secured.

  3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times:
  • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key and is stored separately from the data-encrypting key.
  • Within a secure cryptographic device (SCD), such as an HSM or PTS-approved point-of-interaction device.
  • As at least two full-length key components or key shares, following an industry-accepted method.

  Procedure
  - Examine documented procedures to verify it is defined that cryptographic keys used to encrypt/decrypt stored account data must exist only in one (or more) of the forms specified in this requirement.
  - Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt stored account data exist in one (or more) of the forms specified in this requirement.
  - Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: • 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.

- PCI-3.6.1.3 - Requirement 3.6.1.3:
  Cryptographic keys used to protect stored account data are secured.

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

  Procedure
  - Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest numbers of custodians necessary.

- PCI-3.6.1.4 - Requirement 3.6.1.4:
  Cryptographic keys used to protect stored account data are secured.

  3.6.1.4 Cryptographic keys are stored in the fewest possible locations.

  Procedure
  - Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.

- PCI-3.7.1 - Requirement 3.7.1:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

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

Procedure

- Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define the generation of strong cryptographic keys.
- Observe the method for generating keys to verify that strong keys are generated.

- PCI-3.7.2 - Requirement 3.7.2:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

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

  Procedure
  - Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure distribution of cryptographic keys.
  - Observe the method for distributing keys to verify that keys are distributed securely.

- PCI-3.7.3 - Requirement 3.7.3:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

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

  Procedure
  - Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure storage of cryptographic keys.
  - Observe the method for storing keys to verify that keys are stored securely.

- PCI-3.7.4 - Requirement 3.7.4:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

  3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod.

  Procedure
  - Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define changes to cryptographic keys that have reached the end of their cryptoperiod and include all elements specified in this requirement.
  - Interview personnel, examine documentation, and observe key storage locations to verify that keys are changed at the end of the defined cryptoperiod(s).

- PCI-3.7.5 - Requirement 3.7.5:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

  3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when:
  - The key has reached the end of its defined cryptoperiod.
  - The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known.
  - The key is suspected of or known to be compromised.

  Procedure
  - Examine the documented key management policies and procedures for keys used for protection of stored account data and verify that they define retirement, replacement, or destruction of keys in accordance with all elements specified in this requirement.
  - Interview personnel to verify that processes are implemented in accordance with all elements specified in this requirement.

- PCI-3.7.6 - Requirement 3.7.6:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

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

  Procedure
  - Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define using split knowledge and dual control.
  - Interview personnel and/or observe processes to verify that manual cleartext keys are managed with split knowledge and dual control.

- PCI-3.7.7 - Requirement 3.7.7:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

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

  Procedure
  - Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define prevention of unauthorized substitution of cryptographic keys.
  - Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.

- PCI-3.7.8 - Requirement 3.7.8:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are

defined and implemented.

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

Procedure

- Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define acknowledgments for key custodians in accordance with all elements specified in this requirement.
- Examine documentation or other evidence showing that key custodians have provided acknowledgments in accordance with all elements specified in this requirement.

- PCI-3.7.9 - Requirement 3.7.9:
  Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are
  defined and implemented.

  3.7.9 Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.

  Procedure
  - Additional testing procedure for service provider assessments only: If the service provider shares cryptographic keys with its customers for transmission or storage of account data, examine the documentation that the service provider provides to its customers to verify it includes guidance on how to securely transmit, store, and update customers' keys in accordance with all elements specified in Requirements 3.7.1 through 3.7.8 above.

References

- PCI Security Standards Council Document Library - https://www.pcisecuritystandards.org/document_library/
- PCI Security Standards Council - https://www.pcisecuritystandards.org/
- PCI DSS v4.0 At a Glance - https://www.pcisecuritystandards.org/document_library?category=pcidss&document=dss4aag
- PCI DSS Requirements & Testing Procedure - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Truncated Sample Document