YourIT!
Your Logo Goes Here

PCI DSS - SAQ C

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

1 - Purpose

2 - Scope

3 - Sanctions/Compliance

4 - Requirement 1 - Install and Maintain Network Security Controls

5 - Requirement 2 - Apply Secure Configurations to All System Components

6 - Requirement 3 - Protect Stored Account Data

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

8 - Requirement 5 - Protect All Systems and Networks from Malicious Software

9 - Requirement 6 - Develop and Maintain Secure Systems and Software

10 - Requirement 7 - Restrict Access to System Components and Cardholder Data by Business Need to Know

11 - Requirement 8 - Identify Users and Authenticate Access to System Components

12 - Requirement 9 - Restrict Physical Access to Cardholder Data

13 - Requirement 10 - Log and Monitor All Access to System Components and Cardholder Data

14 - Requirement 11 - Test Security of Systems and Networks Regularly

15 - Requirement 12 - Support Information Security with Organizational Policies and Programs

16 - Appendix A2 - Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections

Purpose

The intended audience for this SAQ includes merchants who process cardholder data through POS systems and do not store such data electronically. This SAQ should be utilized when merchants meet the eligibility criteria outlined in the document, ensuring compliance with PCI DSS requirements specific to their environment. Unique validation requirements include confirming that the payment application system is not connected to other systems and that all applicable PCI DSS requirements are addressed. This SAQ is not suitable for service providers or merchants with e-commerce channels.

Scope

This Self-Assessment Questionnaire (SAQ) C applies to merchants with payment application systems connected to the Internet that do not store electronic account data. It encompasses all system components, personnel, and processes involved in the handling of cardholder data via point-of-sale (POS) systems or other payment applications. The SAQ requires that the payment application system is isolated from other systems through network segmentation, ensuring that no account data is stored electronically. This SAQ differs from others by specifically addressing environments where cardholder data is processed but not stored, excluding e-commerce and service provider scenarios.

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 C	Other Requirements
Requirement 1 Install and Maintain Network Security Controls	N/A

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

1.3 Network access to and from the cardholder data environment is restricted.

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-1.3.1 - 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.

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 C Requirement 2 Apply Secure Configurations to All System Components	Other Requirements 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-2.2.1 - 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 C	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.
3.3 Sensitive authentication data (SAD) is not stored after authorization.
3.4 Access to displays of full PAN and ability to copy PAN are restricted.

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.

SAQ Completion Guidance for SAQ C - Requirement 3

Requirement 3.1.1
If the merchant has paper storage of account data, it must have policies and procedures in place that govern activities related to the secure storage of these records. This ensures that personnel are aware of and follow security policies and documented operational procedures. If the merchant does not store paper records with account data, this requirement should be marked as Not Applicable.

Requirement 3.3.1.2
If the merchant writes down the card verification code during a transaction, it must securely destroy the paper immediately after the transaction or obscure the code before storing the paper. If the merchant never requests the card verification code, this requirement should be marked as Not Applicable.

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-3.3.1.2-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-3.4.1 - 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.

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

PCI DSS - SAQ C Requirement 4 Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Other Requirements N/A

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

4.2 PAN is protected with strong cryptography during transmission

Guidance
Overview
The use of strong cryptography provides greater assurance in preserving data confidentiality, integrity, and non-repudiation.

To protect against compromise, PAN must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals aiming to exploit these vulnerabilities to gain privileged access to cardholder data environments (CDE). Any transmissions of cardholder data over an entity's internal network(s) will naturally bring that network into scope for PCI DSS since that network stores, processes, or transmits cardholder data. Any such networks must be evaluated and assessed against applicable PCI DSS requirements.

Requirement 4 applies to transmissions of PAN unless specifically called out in an individual requirement.

PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is recommended.

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-4.2.1.2 - Requirement 4.2.1.2:
  PAN is protected with strong cryptography during transmission.

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

  Procedure

- Examine system configurations to verify that wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

- PCI-4.2.1-v4.0.1 - Requirement 4.2.1:
  PAN is protected with strong cryptography during transmission.

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

  Procedure
  - Examine documented policies and procedures and interview personnel to verify processes are defined to include all elements specified in this requirement.
  - Examine system configurations to verify that strong cryptography and security protocols are implemented in accordance with all elements specified in this requirement.
  - Examine cardholder data transmissions to verify that all PAN is encrypted with strong cryptography when it is transmitted over open, public networks.

- PCI-4.2.2-v4.0.1 - Requirement 4.2.2:
  PAN is protected with strong cryptography during transmission.

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

  Procedure
  - Examine documented policies and procedures to verify that processes are defined to secure PAN with strong cryptography whenever sent over end-user messaging technologies.
  - Examine system configurations and vendor documentation to verify that PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.

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