PCI DSS – SAQ A

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

Purpose

The intended audience for this SAQ includes merchants who process card-not-present transactions and have no electronic storage, processing, or transmission of account data. This SAQ should be utilized when a merchant's operations meet the eligibility criteria outlined, specifically when all account data functions are outsourced to compliant TPSPs. Unique compliance requirements include confirming TPSP compliance and ensuring that any retained account data is limited to paper records. This SAQ is not applicable for merchants with in-scope systems or those using other payment channels.

Scope

This Self-Assessment Questionnaire (SAQ) A applies to merchants that exclusively accept card-not-present transactions (e-commerce or mail/telephone-order) and have fully outsourced all account data processing to PCI DSS compliant third-party service providers (TPSPs). The scope includes only those system components, processes, and personnel directly involved in the management of paper records containing account data. Merchants must ensure their e-commerce sites are not vulnerable to script attacks and that all payment page elements originate from a compliant TPSP. This SAQ does not cover face-to-face transactions or service providers.

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 2 - Apply Secure Configurations to All System Components

PCI DSS - SAQ A	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:

2.2 System components 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-2.2.2 - 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.

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 A Requirement 3 Protect Stored Account Data	Other Requirements 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.

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 A - Requirement 3

Requirement 3.1.1
If the merchant has paper storage of account data, the merchant has policies and procedures in place that govern merchant activities for Requirement 3. This helps to ensure personnel are aware of and following security policies and documented operational procedures for managing the secure storage of any paper records with account data.
If merchant does not store paper records with account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Requirement 3.2.1
If a merchant stores any paper (for example, receipts or paper reports) that contain account data, the merchant only stores the paper as long as it is needed for business, legal, and/or regulatory reasons and destroys the paper once it is no longer needed.
If a merchant never prints or stores any paper containing account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted 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-3.2.1 - 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.

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 6 - Develop and Maintain Secure Systems and Software

PCI DSS - SAQ A Requirement 6 Develop and Maintain Secure Systems and Software	Other Requirements N/A

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

6.3 Security vulnerabilities are identified and addressed.

Guidance
Overview
Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software.

Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software lifecycle (SLC) processes and secure coding techniques.

Code repositories that store application code, system configurations, or other configuration data that can impact the security of cardholder data and/or sensitive authentication data are in scope for PCI DSS assessments.
See Relationship between PCI DSS and PCI SSC Software Standards on page 7 for information about the use of PCI SSC-validated software and software vendors, and how use of PCI SSC's software standards may help with meeting controls in Requirement 6.

Refer to Appendix G for definitions of PCI DSS terms.

Note: Requirement 6 applies to all system components, except for section 6.2 for developing software securely, which applies only to bespoke and custom software used on any system component included in or connected to the CDE.

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

Related Internal Controls
- PCI-6.3.1-v4.0.1 - Requirement 6.3.1:
  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 information, including alerts from international and national computer emergency response teams (CERTs).

• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Procedure
- Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.
- Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.

- PCI-6.3.3-v4.0.1 - Requirement 6.3.3:
  Security vulnerabilities are identified and addressed.

  6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:
  • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
  • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1.

  Procedure
  - Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement.
  - Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed 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 8 - Identify Users and Authenticate Access to System Components

PCI DSS - SAQ A	Other Requirements
Requirement 8 Identify Users and Authenticate Access to System Components	N/A

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

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.
8.3 Strong authentication for users and administrators is established and managed.

Guidance
Overview
Two fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity is who the user claims to be.

Identification of an individual or process on a computer system is conducted by associating an identity with a person or process through an identifier, such as a user, system, or application ID. These IDs (also referred to as accounts) fundamentally establish the identity of an individual or process by assigning unique identification to each person or process to distinguish one user or process from another. When each user or process can be uniquely identified, it ensures there is accountability for actions performed by that identity. When such accountability is in place, actions taken can be traced to known and authorized users and processes.

The element used to prove or verify the identity is known as the authentication factor. Authentication factors are 1) something you know, such as a password or passphrase, 2) something you have, such as a token device or smart card, or 3) something you are, such as a biometric element.

The ID and the authentication factor together are considered authentication credentials and are used to gain access to the rights and privileges associated with a user, application, system, or service accounts.

These requirements for identity and authentication are based on industry-accepted security principles and best practices to support the payment ecosystem. NIST Special Publication 800-63, Digital Identity Guidelines provides additional information on acceptable frameworks for digital identity and authentication factors. It is important to note that the NIST Digital Identity Guidelines is intended for US Federal Agencies and should be viewed in its entirety. Many of the concepts and approaches defined in these guidelines are expected to work with each other and not as standalone parameters.

Note: Unless otherwise stated in the requirement, these requirements apply to all accounts on all system components, unless specifically called out in an individual requirement, including but not limited to:
- Point-of-sale accounts
- Accounts with administrative capabilities
- System and application accounts
- All accounts used to view or access cardholder data or to access systems with cardholder data.

This includes accounts used by employees, contractors, consultants, internal and external vendors, and other third parties (for example, for providing support or maintenance services).

Certain requirements are 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 single transaction. When items do not apply, they are noted directly within the specific requirement.

These requirements do not apply to accounts used by consumers (cardholders).

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-8.2.1 - Requirement 8.2.1:
  User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

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

  Procedure
  - Interview responsible personnel to verify that all users are assigned a unique ID for access to system components and cardholder data.
  - Examine audit logs and other evidence to verify that access to system components and cardholder data can be uniquely identified and associated with individuals.

- PCI-8.2.2-v4.0.1 - Requirement 8.2.2:
  User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

  8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:
  • ID 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.

  Procedure
  - Examine user account lists on system components and applicable documentation to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.
  - Examine authentication policies and procedures to verify processes are defined for shared authentication credentials such that they are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.
  - Interview system administrators to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.

- PCI-8.2.5 - Requirement 8.2.5:

User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.2.5 Access for terminated users is immediately revoked.

Procedure
- Examine information sources for terminated users and review current user access lists—for both local and remote access—to verify that terminated user IDs have been deactivated or removed from the access lists.
- Interview responsible personnel to verify that all physical authentication factors—such as, smart cards, tokens, etc.—have been returned or deactivated for terminated users.

- PCI-8.3.1 - Requirement 8.3.1:
  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 following authentication factors:
  • 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.

  Procedure
  - Examine documentation describing the authentication factor(s) used to verify that user access to system components is authenticated via at least one authentication factor specified in this requirement.
  - For each type of authentication factor used with each type of system component, observe an authentication to verify that authentication is functioning consistently with documented authentication factor(s).

- PCI-8.3.5 - Requirement 8.3.5:
  Strong authentication for users and administrators is established and managed.

  8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
  • Set to a unique value for first-time use and upon reset.
  • Forced to be changed immediately after the first use.

  Procedure
  - Examine procedures for setting and resetting passwords/passphrases (if used as authentication factors to meet Requirement 8.3.1) and observe security personnel to verify that passwords/passphrases are set and reset in accordance with all elements specified in this requirement.

- PCI-8.3.6 - Requirement 8.3.6:
  Strong authentication for users and administrators is established and managed.

  8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:
  • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
  • Contain both numeric and alphabetic characters.

  Procedure

- Examine system configuration settings to verify that user password/passphrase complexity parameters are set in accordance with all elements specified in this requirement.

- PCI-8.3.7 - Requirement 8.3.7:
  Strong authentication for users and administrators is established and managed.

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

  Procedure
  - Examine system configuration settings to verify that password parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.

- PCI-8.3.9-v4.0.1 - Requirement 8.3.9:
  Strong authentication for users and administrators is established and managed.

  8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in 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 automatically determined accordingly.

  Procedure
  - If passwords/passphrases are used as the only authentication factor for user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the 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

TRUNCATED SAMPLE DOCUMENT