YourIT!
Your Logo Goes Here

PCI DSS - SAQ B-IP

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

Purpose

The intended audience for this SAQ includes brick-and-mortar and mail/telephone-order merchants that exclusively use standalone, PCI-listed approved PTS POI devices for payment processing. This SAQ should be utilized when merchants meet the eligibility criteria outlined in the document and do not engage in e-commerce or store cardholder data electronically. Unique compliance requirements include ensuring that all account data transmission occurs solely from approved devices to the payment processor, with no storage of cardholder data in electronic format.

Scope

This Self-Assessment Questionnaire (SAQ) B-IP applies to merchants that process cardholder data exclusively through standalone, PCI-listed approved Point-of-Interaction (POI) devices with an IP connection to a payment processor. It encompasses all relevant system components, personnel, and processes involved in this payment channel. The SAQ is not applicable to e-commerce transactions or service providers. Merchants must ensure that their POI devices are isolated from other systems through network segmentation and do not store cardholder data electronically. This SAQ differs from others by focusing solely on environments utilizing specific PTS-approved devices.

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 B-IP	Other Requirements
Requirement 1 Install and Maintain Network Security Controls	N/A

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

1.2 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.

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-1.2.3 - 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-1.2.5 - 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-1.3.1 - 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-1.4.3 - 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.

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 B-IP	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.
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-2.2.2 - 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-2.2.7 - 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 B-IP 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.
3.3 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 B-IP - Requirement 3

Requirement 3.1.1
If the merchant has paper storage of account data, it must have documented security policies and operational procedures in place that ensure personnel are aware of and follow the guidelines for managing the secure storage of any paper records with account data. 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-3.3.1.1-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-3.4.1 - 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

Truncated Sample Document