YourIT!
Your Logo Goes Here

PCI DSS - SAQ B-IP

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

33 - PCI DSS 8.2.2 - Group, Shared, or Generic Accounts
34 - PCI DSS 3.3.1.1 - Track Retention
35 - PCI DSS 2.2.7 - Non-Console Administrative Access
36 - PCI DSS 9.4.6 - Hard Copy Destruction
37 - PCI DSS 9.4.1.1 - Backup Media Security
38 - PCI DSS 2.3.1 - Wireless Defaults
39 - PCI DSS 12.8.5 - Third Party Service Provider PCI-DSS Management
40 - PCI DSS 9.5.1 - Point of Interaction (POI) Device List
41 - PCI DSS 12.8.4 - Third Party Service Provider PCI-DSS Compliance Monitoring
42 - PCI DSS 1.2.3 - Network Diagram(s)
43 - PCI DSS 2.2.2 - Vendor Default Accounts
44 - PCI DSS 9.4.3 - Media Sent Outside
45 - PCI DSS 9.4.2 - Media Classification
46 - PCI DSS 6.3.3 - Security Patches and Updates
47 - PCI DSS 3.3.1.3 - Personal Identification Number (PIN) Retention
48 - PCI DSS 8.4.3 - Remote Access Multi-Factor Authentication
49 - PCI DSS 9.2.2 - Physical Access to Network Jacks
50 - PCI DSS 3.3.1 - Sensitive Authentication Data Retention
51 - PCI DSS 12.1.2 - Comprehensive Information Security Policy Review
52 - PCI DSS 3.4.1 - Primary Account Number Masking
53 - PCI DSS 1.3.3 - Wireless Network Security Controls
54 - PCI DSS 12.8.2 - Third Party Service Provider Agreements
55 - PCI DSS 1.3.1 - CDE Inbound Traffic
56 - PCI DSS 9.4.4 - Media Movement Management
57 - PCI DSS 1.3.2 - CDE Outbound Traffic
58 - PCI DSS 3.3 - Sensitive Authentication Data
59 - PCI DSS 12.1.3 - Information Security Responsibilities
60 - PCI DSS 12.10.1 - Incident Response Plan
61 - PCI DSS 12.6.1 - Formal Security Awareness Program
62 - PCI DSS 3.1.1 - Data Protection Policies and Procedures
63 - PCI DSS 3.3.1.2 - Card Verification Code Retention
64 - PCI DSS 8.1.1 - User Identification and Authentication Policies and Procedures
65 - PCI DSS 9.1.1 - Physical Access Policies and Procedures

66 - PCI DSS 12.1.1 - Comprehensive Information Security Policy Requirements

67 - PCI DSS 12.8.1 - Third Party Service Provider List

68 - PCI DSS 9.5 - Point of Interaction (POI) Devices

69 - PCI DSS 8.2 - User Identification Management

70 - PCI DSS 1.4 - Network connections between trusted and untrusted networks are controlled.

71 - PCI DSS 3.4 - Primary Account Number Protection

72 - PCI DSS 8.4 - Multi-Factor Authentication

73 - PCI DSS 12.1 - Comprehensive Information Security Policy

74 - PCI DSS 12.8 - Third Party Service Provider Management

75 - PCI DSS 1.3 - Network access to and from the cardholder data environment is restricted.

76 - PCI DSS A2.1 - POS Terminal SSL and Early TLS

Purpose

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment card account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data

Cardholder Data includes:

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code

Sensitive Authentication Data includes:

- Full track data (magnetic-stripe data or equivalent on a chip)
- Card verification code
- PINs/PIN blocks

Scope

SAQ B-IP APPLICABILITY

Self-Assessment Questionnaire (SAQ) B-IP includes only those PCI DSS requirements applicable to merchants that process account data only via standalone, PCI-listed approved PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor.

An exception applies for PTS POI devices classified as Secure Card Readers (SCR) and Secure Card Readers for PIN (SCRPs); merchants using SCRs or SCRPs are not eligible for this SAQ.

SAQ B-IP merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store account data on any computer system.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

SAQ B-IP merchants confirm that, for this payment channel:
* The merchant uses only standalone, PCI-listed approved PTS POI devices (excludes SCRs and SCRPs) connected via IP to merchant's payment processor to take customers' payment card information;

* The standalone, IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs and SCRPs);

* The standalone, IP-connected PTS POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate PTS POI devices from other systems)

* The only transmission of account data is from the approved PTS POI devices to the payment processor;

* The PTS POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor;

* The merchant does not store account data in electronic format; and

* Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

This SAQ includes only those requirements that apply to a specific type of merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to the cardholder data environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for the merchant's environment.

A merchant using an expired PTS POI device should check with its acquirer or individual payment brands about acceptability of
this SAQ. Refer to PCI's list of PIN Transaction Security Devices with Expired Approvals.

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.

PCI DSS 7.2 - System and Data Access

PCI DSS - SAQ B-IP 7.2 System and Data Access	Other Requirements N/A

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

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

Guidance
A factor to consider when defining access needs is the separation of duties principle. This principle is intended to prevent fraud and misuse or theft of resources. For example, 1) dividing mission- critical functions and information system support functions among different individuals and/or functions, 2) establishing roles such that information system support activities are performed by different functions/individuals (for example, system management, programming, configuration management, quality assurance and testing, and network security), and 3) ensuring security personnel administering access control functions do not also administer audit functions.

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

Related Internal Controls
- PCIDSS-90 - Access Control Model: An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform and job function.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 12.10 - Security Incident Response

PCI DSS - SAQ B-IP 12.10 Security Incident Response	Other Requirements N/A

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

Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

Guidance
An incident could occur at any time, therefore if a person who is trained in incident response and familiar with the entity's plan is available when an incident is detected, the entity's ability to correctly respond to the incident is increased.

The incident response plan should be thorough and contain all the key elements for stakeholders (for example, legal, communications) to allow the entity to respond effectively in the event of a breach that could impact account data. It is important to keep the plan up to date with current contact information of all individuals designated as having a role in incident response. Other relevant parties for notifications may include customers, financial institutions (acquirers and issuers), and business partners.

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

Related Internal Controls
- PCIDSS-213 - Incident Response Plan: A comprehensive incident response plan that meets card brand expectations is maintained.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 9.1 - Physical Access Processes and Mechanisms

PCI DSS - SAQ B-IP 9.1 Physical Access Processes and Mechanisms	Other Requirements N/A

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

Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

Guidance
Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.

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

Related Internal Controls
- PCIDSS-124 - Physical Access Control Systems: Appropriate facility entry controls are in place to restrict physical access to systems in the Cardholder Data Environment.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 9.2 - Physical Access Controls

PCI DSS - SAQ B-IP 9.2 Physical Access Controls	Other Requirements N/A

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

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

Guidance
Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.

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

Related Internal Controls
- PCIDSS-124 - Physical Access Control Systems: Appropriate facility entry controls are in place to restrict physical access to systems in the Cardholder Data Environment.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 2.3 - Wireless Environments

PCI DSS - SAQ B-IP	Other Requirements
2.3 Wireless Environments	N/A

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

Wireless environments are configured and managed securely.

Guidance
Applying secure configurations to wireless environments reduces the means available to an attacker to compromise the system.

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

Related Internal Controls
- PCIDSS-28 - Wireless Defaults: For wireless environments connected to the Cardholder Data Environment or transmitting account data, change all wireless vendor defaults at installation or confirmed they are secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 8.1 - User Identification and Authentication Processes and Mechanisms

PCI DSS - SAQ B-IP 8.1 User Identification and Authentication Processes and Mechanisms	Other Requirements N/A

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

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.

Guidance
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.

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

Related Internal Controls
- PCIDSS-1 - Policies and procedures: All security policies and operational procedures that are identified in each PCI-DSS Requirement are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within each Requirement are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 11.3 - External and Internal Vulnerabilities

PCI DSS - SAQ B-IP	Other Requirements
11.3 External and Internal Vulnerabilities	N/A

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

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

Guidance
Identifying and addressing vulnerabilities promptly reduces the likelihood of a vulnerability being exploited and the potential compromise of a system component or cardholder data.

Vulnerability scans conducted at least every three months provide this detection and identification.

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

Related Internal Controls
- PCIDSS-174 - Wireless Access Point Management: Unauthorized wireless access points are identified and addressed periodically.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 12.6 - Security Awareness Education

PCI DSS - SAQ B-IP	Other Requirements
12.6 Security Awareness Education	N/A

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

Security awareness education is an ongoing activity.

Guidance
If personnel are not educated about their company's information security policies and procedures and their own security responsibilities, security safeguards and processes that have been implemented may become ineffective through unintentional errors or intentional actions.

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

Related Internal Controls
- PCIDSS-202 - Formal Security Awareness Program: Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 2.2 - System components are configured and managed securely.

PCI DSS - SAQ B-IP	Other Requirements
2.2 System components are configured and managed securely.	N/A

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

Configure all system components securely and consistently and in accordance with industry- accepted hardening standards or vendor recommendations.

Guidance
Keeping up to date with current industry guidance will help the entity maintain secure configurations. The specific controls to be applied to a system will vary and should be appropriate for the type and function of the system.

Numerous security organizations have established system-hardening guidelines and recommendations, which advise how to correct common, known weaknesses.

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

Related Internal Controls
- PCIDSS-3 - Configuration and Maintenance: Configuration standards for Network Security Controls rulesets are: • Defined. • Implemented. • Maintained. Customized Approach Objective The way that Network Security Controls are configured and operate are defined and consistently applied.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 9.4 - Media Controls

PCI DSS - SAQ B-IP 9.4 Media Controls	Other Requirements N/A

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

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

Guidance
Note: For SAQ B-IP, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs).

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirements at 9.4 means that the merchant securely stores any paper media with account data, for example by storing the paper in a locked drawer, cabinet, or safe, and that the merchant destroys such paper when no longer needed for business purposes. This includes a written document or policy for employees, so they know how to secure paper with account data and how to destroy the paper when no longer needed.

If the merchant never stores any paper with account data, mark this requirement as Not Applicable and complete Appendix D: Explanation of Requirements Noted as Not Applicable.

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

Related Internal Controls
- PCIDSS-134 - Media Security: All media with cardholder data is physically secured.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 6.3 - Security Vulnerabilities

PCI DSS - SAQ B-IP	Other Requirements
6.3 Security Vulnerabilities	N/A

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

Security vulnerabilities are identified and addressed.

Guidance
Note: For SAQ B-IP, this requirement applies to the merchant's firewall/router devices that connect PTS POI devices to the payment processor.

Identification and management of security vulnerabilities for PTS POI devices are often handled by the merchant's terminal provider or processor. The merchant should contact the entity managing its terminals to understand how this requirement is met and the responsibilities of the merchant and of the entity managing the terminals.

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

Related Internal Controls
- PCIDSS-77 - Security Vulnerability Management: 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 and risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at and minimum, all vulnerabilities considered to be and high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 1.2 - Network Security Controls Configuration and Maintenance

PCI DSS - SAQ B-IP 1.2 Network Security Controls Configuration and Maintenance	Other Requirements N/A

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

The implementation of these configuration standards results in the NSC being configured and managed to properly perform their security function (often referred to as the ruleset).

Guidance
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.

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

Related Internal Controls
- PCIDSS-3 - Configuration and Maintenance: Configuration standards for Network Security Controls rulesets are: • Defined. • Implemented. • Maintained. Customized Approach Objective The way that Network Security Controls are configured and operate are defined and consistently applied.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 11.4 - External and Internal Penetration Testing

PCI DSS - SAQ B-IP	Other Requirements
11.4 External and Internal Penetration Testing	N/A

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

External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

Guidance
Penetration testing is a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to gain access into an environment. Often the tester will chain several types of exploits together with the goal of breaking through layers of defenses. For example, if the tester finds a way to gain access to an application server, the tester will then use the compromised server as a point to stage a new attack based on the resources to which the server has access. In this way, a tester can simulate the techniques used by an attacker to identify areas of potential weakness in the environment. The testing of security monitoring and detection methods—for example, to confirm the effectiveness of logging and file integrity monitoring mechanisms, should also be considered.

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

Related Internal Controls
- CC17.1 - Vulnerability Scans: Scan for vulnerabilities and encryption status in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

References
- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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

Truncated Sample Report