YourIT!
Your Logo Goes Here

PCI DSS - SAQ C

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

165 - PCI DSS 12.8.5 - Third Party Service Provider PCI-DSS Management

166 - PCI DSS 12.10 - Security Incident Response

167 - PCI DSS 12.10.1 - Incident Response Plan

168 - PCI DSS 12.10.3 - Security Response Personnel Availability

169 - 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 C APPLICABILITY

Merchant Eligibility Criteria for Self-Assessment Questionnaire C
Self-Assessment Questionnaire (SAQ) C includes only those PCI DSS requirements applicable to merchants with payment application systems (for example, point-of-sale systems) connected to the Internet, and that do not store electronic account data.

SAQ C merchants process account data via a point-of-sale (POS) system or other payment application systems connected to the Internet, do not store account data on any computer system, and may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

SAQ C merchants confirm that, for this payment channel:

* The merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN);

* The payment application system is not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);

* The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single store only;

* 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.

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

PCI DSS - SAQ C	Other Requirements
1.3 Network access to and from the cardholder data environment is restricted.	N/A

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

Implement Network security controls (NSCs), such as firewalls and other network security technologies, to control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.

Guidance
This requirement aims to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner.

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

Related Internal Controls
- PCIDSS-11 - Restrict Cardholder Data Environment Network Access: Restrict network access to and from 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 1.3.1 - CDE Inbound Traffic

PCI DSS - SAQ C 1.3.1 CDE Inbound Traffic	Other Requirements N/A

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

Defined Approach Requirements

Inbound traffic to the CDE is restricted as follows:
• To only traffic that is necessary.
• All other traffic is specifically denied.

Customized Approach Objective

Unauthorized traffic cannot enter the CDE.

Guidance
Purpose

This requirement aims to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using
services, protocols, or ports in an unauthorized
manner.

Good Practice

All traffic inbound to the CDE, regardless of where it originates, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to ensure traffic is restricted to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content.

Examples

Implementing a rule that denies all inbound and outbound traffic that is not specifically needed— for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.

Defined Approach Testing Procedures

1.3.1.a 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.

1.3.1.b Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.

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

Related Internal Controls

- PCIDSS-12 - Cardholder Data Environment Traffic: Restrict inbound and outbound traffic to the Cardholder Data Environment: • To only traffic that is necessary. • All other traffic is specifically denied.

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 1.3.2 - CDE Outbound Traffic

PCI DSS - SAQ C 1.3.2 CDE Outbound Traffic	Other Requirements N/A

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

Defined Approach Requirements

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

Customized Approach Objective

Unauthorized traffic cannot leave the CDE.

Guidance
Purpose
This requirement aims to prevent malicious individuals and compromised system components within the entity's network from communicating with an untrusted external host.

Good Practice

All traffic outbound from the CDE, regardless of the destination, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content.

Examples

Implementing a rule that denies all inbound and outbound traffic that is not specifically needed— for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.

Defined Approach Testing Procedures

1.3.2.a 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.

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

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

Related Internal Controls

- PCIDSS-12 - Cardholder Data Environment Traffic: Restrict inbound and outbound traffic to the Cardholder Data Environment: • To only traffic that is necessary. • All other traffic is specifically denied.

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 1.3.3 - Wireless Network Security Controls

PCI DSS - SAQ C 1.3.3 Wireless Network Security Controls	Other Requirements N/A

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

Defined Approach Requirements

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.

Customized Approach Objective

Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.

Guidance
Purpose

The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and account data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If NSCs do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.

Defined Approach Testing Procedures

1.3.3 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.

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

Related Internal Controls
- PCIDSS-13 - Wireless Network Security Controls: Installed security controls between all wireless networks and the Cardholder Data Environment, regardless of whether the wireless network is and 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 2.1 - Secure Configuration Processes

PCI DSS - SAQ C 2.1 Secure Configuration Processes	Other Requirements N/A

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

Processes and mechanisms for applying secure configurations to all system components are defined and understood.

Guidance
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.

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

Related Internal Controls
- PCIDSS-21 - Secure Configuration Processes: Implement processes and mechanisms for applying secure configurations to all system components that are defined and understood.

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 2.1.1 - Secure Configuration Policies and Procedures

PCI DSS - SAQ C 2.1.1 Secure Configuration Policies and Procedures	Other Requirements N/A

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

Defined Approach Requirements

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.

Customized Approach Objective

Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

Guidance
Purpose

Requirement 2.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 2. While it is important to define the specific policies or procedures called out in Requirement 2, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle

Definitions

Security policies define the entity's security objectives and principles.

Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Defined Approach Testing Procedures

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.

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

Truncated Sample Report