YourIT!
Your Logo Goes Here

# PCI DSS - SAQ A-EP

## Policies and Procedures




Prepared for:
Client Company
Prepared by:
YourIT Company

# Table of Contents

# 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 A-EP APPLICABILITY
Self-Assessment Questionnaire (SAQ) A-EP includes only those PCI DSS requirements applicable to e- commerce merchants with a website(s) that does not itself receive account data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the customer's account data.

SAQ A-EP merchants are e-commerce merchants that partially outsource their e-commerce payment channel to PCI DSS validated and compliant third parties and do not electronically store, process, or transmit any account data on their systems or premises.

This SAQ is applicable only to e-commerce channels.

This SAQ is not applicable to service providers

SAQ A-EP merchants will confirm that they meet the following eligibility criteria for this payment channel:

The merchant accepts only e-commerce transactions;

All processing of account data, with the exception of the payment page, is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor;

The merchant's e-commerce website does not receive account data but controls how customers, or their account data, are redirected to a PCI DSS compliant TPSP/payment processor;

If the merchant website is hosted by a TPSP, the TPSP is compliant with all applicable PCI DSS requirements (including PCI DSS Appendix A if the TPSP is a multi-tenant hosting provider);

Each element of the payment page(s) delivered to the customer's browser originates from either the merchant's website or a PCI DSS compliant TPSP;

The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;

The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and has confirmed that the TPSP(s) are PCI DSS compliant for the services used by the merchant; 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.

## 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 1.1 - Installing and Maintaining Network Security Controls

| PCI DSS - SAQ A-EP | Other Requirements |
|---|---|
| 1.1<br><br>Installing and Maintaining Network Security Controls | N/A |

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

Processes and mechanisms for installing and maintaining network security controls are defined and understood.

**Guidance**
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.

**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 1.1.1 - Network Security Controls Policies and Procedures

| PCI DSS - SAQ A-EP<br><br>1.1.1<br><br>Network Security Controls Policies and Procedures | Other Requirements<br>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 1 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 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

**Guidance**
Purpose

Requirement 1.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 1. While it is important to define the specific policies or procedures called out in Requirement 1, 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 these reasons, 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 1 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

# PCI DSS 1.2 - Network Security Controls Configuration and Maintenance

| PCI DSS - SAQ A-EP<br><br>1.2<br><br>Network Security Controls Configuration and Maintenance | Other Requirements<br>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 1.2.1 - Network Security Controls Configuration Standards

| PCI DSS - SAQ A-EP<br><br>1.2.1<br><br>Network Security Controls Configuration Standards | Other Requirements<br>N/A |
|---|---|

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

Defined Approach Requirements

Configuration standards for NSC rulesets are:
• Defined.
• Implemented.
• Maintained.

Customized Approach Objective

The way that NSCs are configured and operate are defined and consistently applied.

**Guidance**
Purpose
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).

Good Practice

These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network.

Definitions

NSCs are key components of a network architecture. Most commonly, NSCs are used at the boundaries of the CDE to control network traffic flowing inbound and outbound from the CDE.

Configuration standards outline an entity's minimum requirements for the configuration of its NSCs

Examples

Examples of NSCs covered by these configuration standards include, but are not limited to, firewalls, routers configured with access control lists, and cloud virtual networks.

Defined Approach Testing Procedures

1.2.1.a Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement.

1.2.1.b Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.

**Responsibilities**

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

**Related Internal Controls**

- PCIDSS-4 - Configuration Standards: Configuration standards for PCI-DSS Requirements are: • Defined. • Implemented. • 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 1.2.2 - Network Connection and Configuration Changes

| PCI DSS - SAQ A-EP<br><br>1.2.2<br><br>Network Connection and Configuration Changes | Other Requirements<br>N/A |
|---|---|

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

Defined Approach Requirements

All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.

Customized Approach Objective

Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.

Applicability Notes

Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.

**Guidance**
Good Practice
Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Verification should provide reasonable assurance that the change did not adversely impact the security of the network and that the change performs as expected.

To avoid having to address security issues introduced by a change, all changes should be approved prior to being implemented and verified after the change is implemented. Once approved and verified, network documentation should be updated to include the changes to prevent inconsistencies between network documentation and the actual configuration.

Defined Approach Testing Procedures

1.2.2.a Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.

1.2.2.b Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.

1.2.2.c Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.

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

**Related Internal Controls**
- PCIDSS-5 - Change Controls: All changes are approved and managed in accordance with the change control process defined at Requirement 6.5.1.

**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 1.2.3 - Network Diagram(s)

| PCI DSS - SAQ A-EP<br><br>1.2.3<br><br>Network Diagram(s) | Other Requirements<br>N/A |
|---|---|

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

Defined Approach Requirements

An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.

Customized Approach Objective

A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.

Applicability Notes

A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.

**Guidance**
Purpose

Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise. A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE.

Good Practice

All connections to and from the CDE should be identified, including systems providing security, management, or maintenance services to CDE system components. Entities should consider including the following in their network diagrams:
• All locations, including retail locations, data centers, corporate locations, cloud providers, etc.
• Clear labeling of all network segments.
• All security controls providing segmentation, including unique identifiers for each control (for example, name of control, make, model, and version).
• All in-scope system components, including NSCs, web app firewalls, anti-malware solutions, change management solutions, IDS/IPS, log aggregation systems, payment terminals, payment applications, HSMs, etc.
• Clear labeling of any out-of-scope areas on the diagram via a shaded box or other mechanism.
• Date of last update, and names of people that made and approved the updates.
• A legend or key to explain the diagram.

Diagrams should be updated by authorized personnel to ensure diagrams continue to provide an accurate description of the network.

Defined Approach Testing Procedures

1.2.3.a Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement.

1.2.3.b Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.

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

**Related Internal Controls**
- PCIDSS-6 - Network Diagrams: Maintain and accurate and up-to-date network diagram(as) to prevent network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise.

**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**