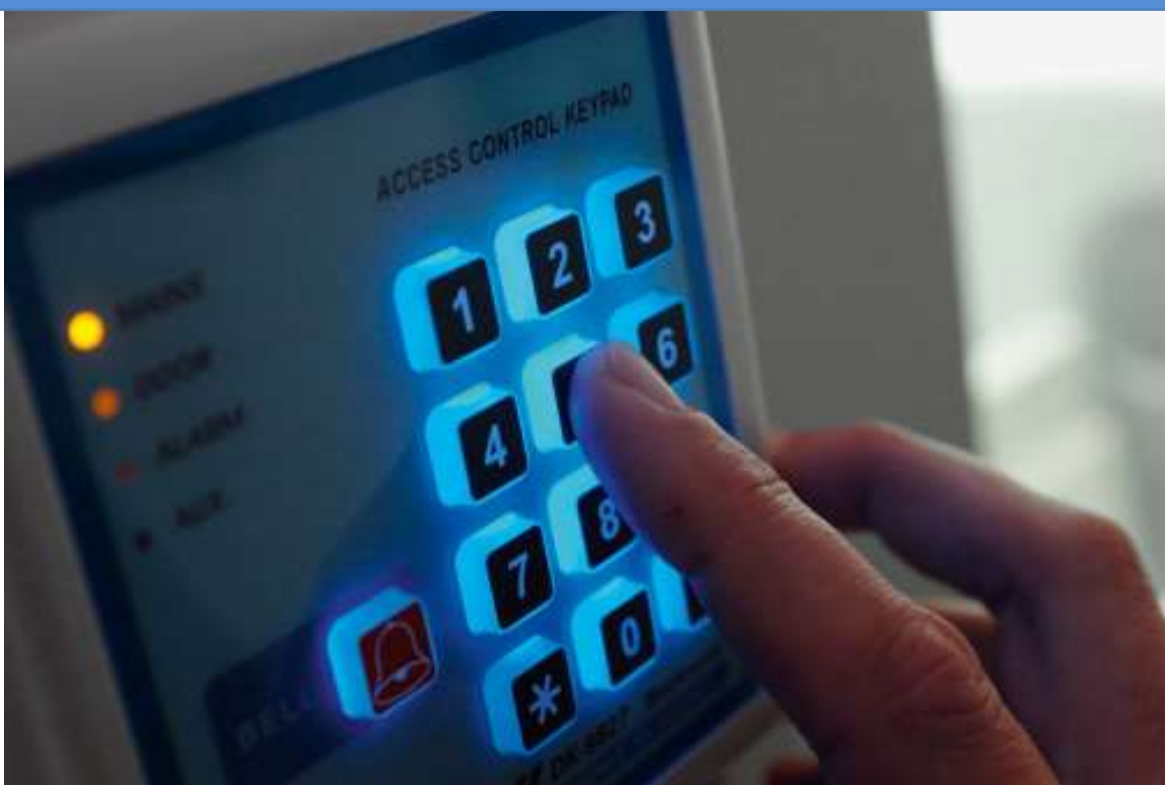




PCI DSS - SAQ C

Policies and Procedures



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

- 1 - Purpose
- 2 - Scope
- 3 - Sanctions/Compliance
- 4 - PCI DSS 1.3 - Network access to and from the cardholder data environment is restricted.
- 5 - PCI DSS 1.3.1 - CDE Inbound Traffic
- 6 - PCI DSS 1.3.2 - CDE Outbound Traffic
- 7 - PCI DSS 1.3.3 - Wireless Network Security Controls
- 8 - PCI DSS 2.1 - Secure Configuration Processes
- 9 - PCI DSS 2.1.1 - Secure Configuration Policies and Procedures
- 10 - PCI DSS 2.2 - System components are configured and managed securely.
- 11 - PCI DSS 2.2.1 - Configuration Standards
- 12 - PCI DSS 2.2.2 - Vendor Default Accounts
- 13 - PCI DSS 2.2.3 - Primary Functions
- 14 - PCI DSS 2.2.4 - Necessary Services
- 15 - PCI DSS 2.2.5 - Insecure Services
- 16 - PCI DSS 2.2.6 - System Security Parameters
- 17 - PCI DSS 2.2.7 - Non-Console Administrative Access
- 18 - PCI DSS 2.3 - Wireless Environments
- 19 - PCI DSS 2.3.1 - Wireless Defaults
- 20 - PCI DSS 2.3.2 - Wireless Encryption Keys
- 21 - PCI DSS 3.1 - Protecting Stored Account Data
- 22 - PCI DSS 3.1.1 - Data Protection Policies and Procedures
- 23 - PCI DSS 3.3 - Sensitive Authentication Data
- 24 - PCI DSS 3.3.1 - Sensitive Authentication Data Retention
- 25 - PCI DSS 3.3.1.2 - Card Verification Code Retention
- 26 - PCI DSS 3.3.1.3 - Personal Identification Number (PIN) Retention
- 27 - PCI DSS 3.4 - Primary Account Number Protection
- 28 - PCI DSS 3.4.1 - Primary Account Number Masking
- 29 - PCI DSS 4.2 - Primary Account Number Transmission Cryptography
- 30 - PCI DSS 4.2.1 - Primary Account Number Public Network Safeguards
- 31 - PCI DSS 4.2.1.2 - Primary Account Number Wireless Networks
- 32 - PCI DSS 4.2.2 - Primary Account Number Messaging Cryptography



- 33 - PCI DSS 5.1 - Malicious Software Protection Processes and Mechanisms
- 34 - PCI DSS 5.1.1 - Malicious Software Protection Policies and Procedures
- 35 - PCI DSS 5.2 - Malware Prevention, Detection, and Response
- 36 - PCI DSS 5.2.1 - Malware Protection
- 37 - PCI DSS 5.2.2 - Malware Detection and Removal
- 38 - PCI DSS 5.2.3 - Malicious Software Evaluation
- 39 - PCI DSS 5.2.3.1 - Malware Risk Analysis Frequency
- 40 - PCI DSS 5.3 - Anti-Malware Mechanisms and Processes
- 41 - PCI DSS 5.3.1 - Anti-Malware Updates
- 42 - PCI DSS 5.3.2 - Anti-Malware Scanning or Analysis
- 43 - PCI DSS 5.3.2.1 - Malware Scan Frequency
- 44 - PCI DSS 5.3.3 - Removable Media Malware Scan or Analysis
- 45 - PCI DSS 5.3.4 - Anti-Malware Audit Logs
- 46 - PCI DSS 5.3.5 - Anti-Malware Disabling
- 47 - PCI DSS 5.4 - Anti-Phishing Mechanisms
- 48 - PCI DSS 5.4.1 - Phishing Attack Detection and Protection
- 49 - PCI DSS 6.2 - Custom Software
- 50 - PCI DSS 6.2.1 - Custom Software Security
- 51 - PCI DSS 6.2.2 - Custom Software Personnel Training
- 52 - PCI DSS 6.2.3.1 - Custom Software Manual Code Review
- 53 - PCI DSS 6.2.4 - Software Engineering Techniques
- 54 - PCI DSS 6.3 - Security Vulnerabilities
- 55 - PCI DSS 6.3.1 - Security Vulnerability Management
- 56 - PCI DSS 6.3.3 - Security Patches and Updates
- 57 - PCI DSS 6.5 - Change Management
- 58 - PCI DSS 6.5.1 - Change Management Procedures
- 59 - PCI DSS 6.5.2 - Change Management Confirmation and Documentation
- 60 - PCI DSS 7.2 - System and Data Access
- 61 - PCI DSS 7.2.2 - Access Assignments
- 62 - PCI DSS 7.2.3 - Access Privileges
- 63 - PCI DSS 7.2.4 - Account and Privilege Reviews
- 64 - PCI DSS 7.2.5 - Application and System Account Assignments
- 65 - PCI DSS 8.1 - User Identification and Authentication Processes and Mechanisms



- 66 - [PCI DSS 8.1.1 - User Identification and Authentication Policies and Procedures](#)
- 67 - [PCI DSS 8.2 - User Identification Management](#)
- 68 - [PCI DSS 8.2.1 - Unique User ID](#)
- 69 - [PCI DSS 8.2.2 - Group, Shared, or Generic Accounts](#)
- 70 - [PCI DSS 8.2.4 - User ID and Authentication Factors](#)
- 71 - [PCI DSS 8.2.5 - Access Termination](#)
- 72 - [PCI DSS 8.2.6 - Inactive User Accounts](#)
- 73 - [PCI DSS 8.2.7 - Third Party Access Management](#)
- 74 - [PCI DSS 8.2.8 - Session Time-Outs](#)
- 75 - [PCI DSS 8.3 - Strong Authentication](#)
- 76 - [PCI DSS 8.3.1 - Strong Authentication Factors](#)
- 77 - [PCI DSS 8.3.2 - Authentication Factor Cryptography](#)
- 78 - [PCI DSS 8.3.3 - User Identity Verification](#)
- 79 - [PCI DSS 8.3.4 - Invalid Authentication Attempts](#)
- 80 - [PCI DSS 8.3.5 - Passwords/Passphrases](#)
- 81 - [PCI DSS 8.3.6 - Password/Passphrase Complexity](#)
- 82 - [PCI DSS 8.3.7 - Password/Passphrase Re-use](#)
- 83 - [PCI DSS 8.3.8 - Authentication Policies and Procedures](#)
- 84 - [PCI DSS 8.3.9 - Password/Passphrase Changes](#)
- 85 - [PCI DSS 8.4 - Multi-Factor Authentication](#)
- 86 - [PCI DSS 8.4.1 - CDE Administrative User Access](#)
- 87 - [PCI DSS 8.4.2 - Multi-Factor Authentication CDE Access](#)
- 88 - [PCI DSS 8.4.3 - Remote Access Multi-Factor Authentication](#)
- 89 - [PCI DSS 8.5 - Multi-Factor Authentication Configuration](#)
- 90 - [PCI DSS 8.5.1 - Multi-Factor Authentication System Implementation](#)
- 91 - [PCI DSS 8.6 - Application and System Account Authentication Factors](#)
- 92 - [PCI DSS 8.6.1 - Interactive Logins](#)
- 93 - [PCI DSS 8.6.2 - Interactive Login Passwords/Passphrases](#)
- 94 - [PCI DSS 8.6.3 - Application and System Account Passwords/Passphrases](#)
- 95 - [PCI DSS 9.1 - Physical Access Processes and Mechanisms](#)
- 96 - [PCI DSS 9.1.1 - Physical Access Policies and Procedures](#)
- 97 - [PCI DSS 9.2 - Physical Access Controls](#)
- 98 - [PCI DSS 9.2.1 - Physical Access Control Systems](#)

- 99 - [PCI DSS 9.2.1.1 - Physical Access Monitoring](#)
- 100 - [PCI DSS 9.2.2 - Physical Access to Network Jacks](#)
- 101 - [PCI DSS 9.4 - Media Controls](#)
- 102 - [PCI DSS 9.4.1 - Media Security](#)
- 103 - [PCI DSS 9.4.1.1 - Backup Media Security](#)
- 104 - [PCI DSS 9.4.2 - Media Classification](#)
- 105 - [PCI DSS 9.4.3 - Media Sent Outside](#)
- 106 - [PCI DSS 9.4.4 - Media Movement Management](#)
- 107 - [PCI DSS 9.4.6 - Hard Copy Destruction](#)
- 108 - [PCI DSS 9.5 - Point of Interaction \(POI\) Devices](#)
- 109 - [PCI DSS 9.5.1 - Point of Interaction \(POI\) Device Protection](#)
- 110 - [PCI DSS 9.5.1.1 - Point of Interaction \(POI\) Device List](#)
- 111 - [PCI DSS 9.5.1.2 - Point of Interaction \(POI\) Device Inspection](#)
- 112 - [PCI DSS 9.5.1.3 - Personnel Training](#)
- 113 - [PCI DSS 10.1 - Access Logging and Monitoring Processes and Mechanisms](#)
- 114 - [PCI DSS 10.1.1 - Access Logging and Monitoring Policies and Procedures](#)
- 115 - [PCI DSS 10.2 - Audit Logs](#)
- 116 - [PCI DSS 10.2.1.2 - Administrative User Access Logs](#)
- 117 - [PCI DSS 10.2.1.4 - Invalid Access Audit Logs](#)
- 118 - [PCI DSS 10.2.1.5 - Change Audit Logs](#)
- 119 - [PCI DSS 10.2.2 - Audit Log Contents](#)
- 120 - [PCI DSS 10.3 - Audit Log Protection](#)
- 121 - [PCI DSS 10.3.1 - Audit Log Read Access](#)
- 122 - [PCI DSS 10.3.2 - Audit Log Modification Protection](#)
- 123 - [PCI DSS 10.3.3 - Audit log Backups](#)
- 124 - [PCI DSS 10.3.4 - Audit log Integrity](#)
- 125 - [PCI DSS 10.4 - Audit log Reviews](#)
- 126 - [PCI DSS 10.4.1 - Audit Log Review Process](#)
- 127 - [PCI DSS 10.4.1.1 - Automated Audit Log Reviews](#)
- 128 - [PCI DSS 10.4.2 - Periodic Audit Log Reviews](#)
- 129 - [PCI DSS 10.4.2.1 - Audit Log Review Frequency](#)
- 130 - [PCI DSS 10.4.3 - Audit Log Review Exceptions and Anomalies](#)
- 131 - [PCI DSS 10.5 - Audit Log History](#)



- 132 - [PCI DSS 10.5.1 - Audit Log History Retention](#)
- 133 - [PCI DSS 10.6 - Time-synchronization](#)
- 134 - [PCI DSS 10.6.1 - System Clock Synchronization](#)
- 135 - [PCI DSS 10.6.2 - Time Accuracy](#)
- 136 - [PCI DSS 10.6.3 - Time Synchronization Settings Protection](#)
- 137 - [PCI DSS 11.2 - Wireless Access Points](#)
- 138 - [PCI DSS 11.2.1 - Wireless Access Point Management](#)
- 139 - [PCI DSS 11.2.2 - Wireless Access Point Inventory](#)
- 140 - [PCI DSS 11.3 - External and Internal Vulnerabilities](#)
- 141 - [PCI DSS 11.3.1 - Internal Vulnerability Scan Requirements](#)
- 142 - [PCI DSS 11.3.1.3 - Vulnerability Scans After Changes](#)
- 143 - [PCI DSS 11.3.2 - External Vulnerability Scan Requirements](#)
- 144 - [PCI DSS 11.3.2.1 - External Vulnerability Scan after Changes](#)
- 145 - [PCI DSS 11.4 - External and Internal Penetration Testing](#)
- 146 - [PCI DSS 11.4.5 - Network Segment Penetration Test](#)
- 147 - [PCI DSS 11.5 - Network Intrusion and File Change Detection and Response](#)
- 148 - [PCI DSS 11.5.2 - Change Detection](#)
- 149 - [PCI DSS 12.1 - Comprehensive Information Security Policy](#)
- 150 - [PCI DSS 12.1.1 - Comprehensive Information Security Policy Requirements](#)
- 151 - [PCI DSS 12.1.2 - Comprehensive Information Security Policy Review](#)
- 152 - [PCI DSS 12.1.3 - Information Security Responsibilities](#)
- 153 - [PCI DSS 12.2 - Acceptable Use Policies](#)
- 154 - [PCI DSS 12.2.1 - Acceptable Use Policies Requirements](#)
- 155 - [PCI DSS 12.3 - Risk Identification, Evaluation, and Management](#)
- 156 - [PCI DSS 12.3.1 - Risk Analysis Requirements](#)
- 157 - [PCI DSS 12.6 - Security Awareness Education](#)
- 158 - [PCI DSS 12.6.1 - Formal Security Awareness Program](#)
- 159 - [PCI DSS 12.6.3.1 - Threat and Vulnerability Training](#)
- 160 - [PCI DSS 12.8 - Third Party Service Provider Management](#)
- 161 - [PCI DSS 12.8.1 - Third Party Service Provider List](#)
- 162 - [PCI DSS 12.8.2 - Third Party Service Provider Agreements](#)
- 163 - [PCI DSS 12.8.3 - Third Party Service Provider Due Diligence](#)
- 164 - [PCI DSS 12.8.4 - Third Party Service Provider PCI-DSS Compliance Monitoring](#)



- 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	Other Requirements
1.3.1 CDE Inbound Traffic	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	Other Requirements
1.3.3	N/A
Wireless Network Security Controls	

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	Other Requirements
2.1 Secure Configuration Processes	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	Other Requirements
2.1.1 Secure Configuration Policies and Procedures	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