YourIT!
Your Logo Goes Here

PCI DSS - SAQ C-VT

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 C-VT APPLICABILITY
Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.Not applicable to e-commerce channels.

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing — including merchants, processors, acquirers, issuers, and other service providers.

Whether any entity is required to comply with or validate their compliance to PCI DSS is at the discretion of those organizations that manage compliance programs (such as payment brands and acquirers). Contact the organizations of interest for any additional criteria.

PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of the CDE. Some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data – for example, entities that outsource payment operations or management of their CDE 1. Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.

The primary account number (PAN) is the defining factor for cardholder data. The term account data therefore covers the following: the full PAN, any other elements of cardholder data that are present with the PAN, and any elements of sensitive authentication data.

If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the CDE, they must be protected in accordance with the PCI DSS requirements applicable to cardholder data.

If an entity stores, processes, or transmits PAN, then a CDE exists to which PCI DSS requirements will apply. Some requirements may not be applicable, for example if the entity does not store PAN, then the requirements relating to the protection of stored PAN in Requirement 3 will not be applicable to the entity.

Even if an entity does not store, process, or transmit PAN, some PCI DSS requirements may still apply. Consider the following:

If the entity stores SAD, requirements specifically related to SAD storage in Requirement 3 will be applicable.

If the entity engages third-party service providers to store, process or transmit PAN on its behalf, requirements related to the management of service providers in Requirement 12 will be applicable.

If the entity can impact the security of a CDE because the security of an entity’s infrastructure can affect how cardholder data is processed (for example, via a web server that controls the generation of a payment form or page) some requirements will be applicable.

If cardholder data is only present on physical media (for example paper), requirements relating to the security and disposal of physical media in Requirement 9 will be applicable.

Requirements related to an incident response plan are applicable to all entities, to ensure that there are procedures to follow in the event of a suspected or actual breach of the confidentiality of cardholder data.

Segmentation (or isolation) of the CDE from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce the:

Scope of the PCI DSS assessment

Cost of the PCI DSS assessment

Cost and difficulty of implementing and maintaining PCI DSS controls

Risk to an organization relative to payment card account data (reduced by consolidating that data into fewer, more controlled locations)

Without adequate segmentation (sometimes called a "flat network"), the entire network is in scope for the PCI DSS assessment. Segmentation can be achieved using a number of physical or logical methods, such as properly configured internal network security controls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network. To be considered out of scope for PCI DSS, a system component must be properly segmented (isolated) from the CDE, such that the out-of-scope system component could not impact the security of the CDE, even if that component was compromised.

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-VT	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-VT 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-VT 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-VT 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 1.5 - Risk Mitigation

PCI DSS - SAQ C-VT	Other Requirements
1.5 Risk Mitigation	N/A

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

Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Guidance
Computing devices that are allowed to connect to the Internet from outside the corporate environment—for example, desktops, laptops, tablets, smartphones, and other mobile computing devices used by employees—are more vulnerable to Internet-based threats.

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

Related Internal Controls
- PCIDSS-19 - Network Security Control Implementation: Implemented security controls on and computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and 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 1.5.1 - Network Security Control Implementation

PCI DSS - SAQ C-VT 1.5.1 Network Security Control Implementation	Other Requirements N/A

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

Defined Approach Requirements

Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows:
• Specific configuration settings are defined to prevent threats being introduced into the entity's network.
• Security controls are actively running.
• Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

Customized Approach Objective

Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.

Applicability Notes

These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.

Guidance
Purpose

Computing devices that are allowed to connect to the Internet from outside the corporate environment—for example, desktops, laptops, tablets, smartphones, and other mobile computing devices used by employees—are more vulnerable to Internet-based threats.

Use of security controls such as host-based controls (for example, personal firewall software or end-point protection solutions), network-based security controls (for example, firewalls, network-based heuristics inspection, and malware simulation), or hardware, helps to protect devices from Internet-based attacks, which could use the device to gain access to the organization's systems and data when the device reconnects to the network.

Good Practice

The specific configuration settings are determined by the entity and should be consistent with its network security policies and procedures.

Where there is a legitimate need to temporarily disable security controls on a company-owned or employee-owned device that connects to both an untrusted network and the CDE—for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action is understood and approved by an appropriate management representative. Any disabling or altering of these security controls, including on administrators' own devices, is performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable security controls on their own computers, but there should be alerting mechanisms in place when such controls are disabled and follow up that occurs to ensure processes were followed.

Examples

Practices include forbidding split-tunneling of VPNs for employee-owned or corporate-owned mobile devices and requiring that such devices boot up into a VPN.

Defined Approach Testing Procedure

1.5.1.a Examine policies and configuration standards and interview personnel to verify security controls for computing devices that connect to both untrusted networks, and the CDE, are implemented in accordance with all elements specified in this requirement.

1.5.1.b Examine configuration settings on computing devices that connect to both untrusted networks and the CDE to verify settings are implemented 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-19 - Network Security Control Implementation: Implemented security controls on and computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and 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 2.1 - Secure Configuration Processes

PCI DSS - SAQ C-VT 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-VT 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