AP 8.710, Credit Card Administration – Appendix A

Summary of PCI DSS v4.0 Requirements 1-12

Source: PCI SSC – PCI DSS v4.0 Quick Reference Guide
https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf

Summary of PCI DSS v4.0 Requirements 1-12

Build and Maintain a Secure Network and Systems

In the past, theft of financial records required a criminal to physically enter an entity's business site. Now, payment transactions occur with many different electronic devices, including traditional payment terminals, mobile devices, and other Internet connected computer systems. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing payment account data.

Requirement 1: Install and maintain network security controls

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. Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

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

1.2 Network security controls (NSCs) are configured and maintained.

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

1.4 Network connections between trusted and untrusted networks are controlled.

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

Requirement 2: Apply secure configurations to all system components

Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise systems. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

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

2.2 System components are configured and managed securely.

2.3 Wireless environments are configured and managed securely.

Protect Account Data

Payment account data refers to any information printed, processed, transmitted, or stored in any form on a payment card. Account data refers to both cardholder data and sensitive authentication data, and protection of the account data is required where account data is stored, processed, or transmitted. Entities accepting payment cards are expected to protect account data and to prevent its unauthorized use – whether the data is printed or stored locally, or transmitted over an internal or public network to a remote server or service provider.

Requirement 3: Protect stored account data

Payment account data should not be stored unless it is necessary to meet the needs of the business. Sensitive authentication data must never be stored after authorization. If your organization stores PAN, it is crucial to render it unreadable. If your company stores sensitive authentication data prior to completior of authorization, that data must also be protected[1].

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

3.2 Storage of account data is kept to a minimum.

3.3 Sensitive authentication data (SAD) is not stored after authorization.

3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.

3.5 Primary account number (PAN) is secured wherever it is stored.

3.6 Cryptographic keys used to protect stored account data are secured.

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

---

1 This requirement is a best practice until 31 March 2025, after which it must be fully considered as part of a PCI DSS assessment.

Elements of Account Data and Storage Requirements

Table 3 in PCI DSS (see below) identifies the elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be rendered unreadable – for example, with strong cryptography – when stored. This table is not exhaustive and is presented to illustrate only how the stated requirements apply to the different data elements.

		Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable
Account Data	Cardholder Data	Primary Account Number (PAN)	Storage is kept to a minimum as defined in Requirement 3.2	Yes, as defined in Requirement 3.5
		Cardholder Name	Storage is kept to a minimum as defined in Requirement 3.2[2]	No
		Service Code		
		Expiration Date		
	Sensitive Authentication Data	Full Track Data	Cannot be stored after authorization as defined in Requirement 3.3.1[3]	Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2
		Card verification code		
		PIN/PIN Block		

2 Where data exists in the same environment as PAN.

3 Except as permitted for issuers and companies that support issuing services. Requirements for issuers and issuing services are separately defined in Requirement 3.3.3.

Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks

To protect against compromise, primary account numbers (PANs) must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals aiming to exploit these vulnerabilities to gain privileged access to cardholder data environments (CDE). PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both.

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

4.2 PAN is protected with strong cryptography during transmission.

Maintain a Vulnerability Management Program

Vulnerability management is the process of systematically and continuously finding and mitigating weaknesses in an entity's payment card environment. This includes addressing threats from malicious software, routinely identifying and patching vulnerabilities, and ensuring that software is developed securely and without known coding vulnerabilities.

Requirement 5: Protect all systems and networks from malicious software

Malicious software (malware) is software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system. Examples include viruses, worms, Trojans, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links. Malware can enter the network during many business-approved activities, including employee e-mail (for example, via phishing) and use of the internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities.

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

5.2 Malicious software (malware) is prevented, or detected and addressed.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

Requirement 6: Develop and maintain secure systems and software

Security vulnerabilities in systems and applications may allow criminals to access payment data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All system components must have the most recently released critical security patches installed to prevent exploitation. Entities must also apply patches to less-critical systems in an appropriate timeframe, based on a formal risk analysis. Applications must be developed according to secure development and coding practices, and changes to systems in the cardholder data environment must follow change control procedures.

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

Implement Strong Access Control Measures

Access to payment account data must be granted only on a business need-to-know basis. Logical access controls are technical means used to permit or deny access to data on computer systems. Physical access controls entail the use of locks or other physical means to restrict access to computer media, paper-based records, and computer systems.

Requirement 7: Restrict access to cardholder data by business need-to-know

Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" refers to providing access to only the least amount of data needed to perform a job. "Least privileges" refers to providing only the minimum level of privileges needed to perform a job.

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood

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

7.3 Access to system components and data is managed via an access control system(s).

Requirement 8: Identify users and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Unless otherwise stated in the requirement, these requirements apply to all accounts, including point-of-sale accounts, those with administrative capabilities, and all accounts used to view or access payment account data or systems with those data. These requirements do not apply to accounts used by consumers (cardholders).

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.

Requirement 9: Restrict physical access to cardholder data

Physical access to cardholder data or systems that store, process, or transmit cardholder data should be restricted so that unauthorized individuals cannot access or remove systems or hardcopies containing this data.

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

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

9.3 Physical access for personnel and visitors is authorized and managed.

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

9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

Regularly Monitor and Test Networks

Physical, virtual, and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment applications and payment account data. To prevent exploitation, entities must regularly monitor and test networks to find and address unexpected access and activities, security system failures, and vulnerabilities.

Requirement 10: Log and monitor all access to system components and cardholder data

Logging mechanisms and the ability to track user activities are critical for detection of anomalies and suspicious activities, and for effective forensic analysis. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs.

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

Requirement 11: Test security of systems and networks regularly

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and bespoke and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

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

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

11.5 Network intrusions and unexpected file changes are detected and responded to.

11.6 Unauthorized changes on payment pages are detected and responded to.

TIPS FOR SCANNING

Get Advice. Ask your acquiring bank about any partnerships they may have with PCI Approved Scanning Vendors (ASVs).

Talk to a PCI ASV. See PCI Council website for the list of PCI ASVs.

Select an ASV. Contact several PCI ASVs and select a suitable program.

Address Vulnerabilities. Ask your PCI ASV for help correcting issues found by scanning.

Maintain an Information Security Policy

A strong security policy sets the tone for security affecting an entity's entire company, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of payment account data and their responsibilities for protecting it.

Requirement 12: Support information security with organizational policies and programs

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.4 PCI DSS compliance is managed.

12.5 PCI DSS scope is documented and validated.

12.6 Security awareness education is an ongoing activity.

12.7 Personnel are screened to reduce risks from insider threats.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

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