Purpose

The purpose of this policy is to establish guidelines for maintaining the security and integrity of cardholder data in compliance with the Payment Card Industry Data Security Standard (PCI DSS).

**Scope**

This policy applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

Approval

This policy has been approved by the Organization’s security requirements and the PCI-DSS 4.0.1 security requirements. Policy is effective as of the date indicated below.

**Effective Date**: Date

**Approved By**: Name/Title

Review, Update, and Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description of Change** | **Approved By** |
| 1.0 | 6/2/2024 | Initial Draft. | MC3 Technologies |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Purpose 1](#_Toc171071862)

[Approval 1](#_Toc171071863)

[Review, Update, and Version Control 1](#_Toc171071864)

[PCI Data Security Standard Overview 3](#_Toc171071865)

[PCI Data Security Standard Policy 4](#_Toc171071866)

[Requirement 1: Install and Maintain Network Security Controls 4](#_Toc171071867)

[Purpose 4](#_Toc171071868)

[Scope 4](#_Toc171071869)

[1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood. 4](#_Toc171071870)

[1.2 Network security controls (NSCs) are configured and maintained. 4](#_Toc171071871)

[1.3 Network access to and from the cardholder data environment is restricted. 4](#_Toc171071872)

[1.4 Network connections between trusted and untrusted networks are controlled. 4](#_Toc171071873)

[1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. 5](#_Toc171071874)

[Requirement 2: Apply Secure Configurations to All System Components 6](#_Toc171071875)

[Purpose 6](#_Toc171071876)

[Scope 6](#_Toc171071877)

[2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood. 6](#_Toc171071878)

[2.2 System components are configured and managed securely. 6](#_Toc171071879)

[2.3 Wireless environments are configured and managed securely. 6](#_Toc171071880)

[Requirement 3: Protect Stored Account Data 7](#_Toc171071881)

[Purpose 7](#_Toc171071882)

[Scope 7](#_Toc171071883)

[3.1 Processes and mechanisms for protecting stored account data are defined and understood. 7](#_Toc171071884)

[3.2 Storage of account data is kept to a minimum. 7](#_Toc171071885)

[3.3 Sensitive authentication data (SAD) is not stored after authorization. 7](#_Toc171071886)

[3.4 Access to displays of full PAN and ability to copy PAN are restricted. 7](#_Toc171071887)

[3.5 Primary account number (PAN) is secured wherever it is stored. 7](#_Toc171071888)

[3.6 Cryptographic keys used to protect stored account data are secured. 8](#_Toc171071889)

[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. 8](#_Toc171071890)

[Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over, Open, Public Networks 9](#_Toc171071891)

[Purpose 9](#_Toc171071892)

[Scope 9](#_Toc171071893)

[4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood. 9](#_Toc171071894)

[4.2 PAN is protected with strong cryptography during transmission 9](#_Toc171071895)

[Requirement 5: Protect All Systems and Networks from Malicious Software 10](#_Toc171071896)

[Purpose 10](#_Toc171071897)

[Scope 10](#_Toc171071898)

[5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood. 10](#_Toc171071899)

[5.2 Malicious software (malware) is prevented or detected and addressed. 10](#_Toc171071900)

[5.3 Anti-malware mechanisms and processes are active, maintained, and monitored. 10](#_Toc171071901)

[5.4 Anti-phishing mechanisms protect users against phishing attacks. 10](#_Toc171071902)

[Requirement 6: Develop and Maintain Secure Systems and Software 11](#_Toc171071903)

[Purpose 11](#_Toc171071904)

[Scope 11](#_Toc171071905)

[6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood. 11](#_Toc171071906)

[6.2 Bespoke and custom software are developed securely. 11](#_Toc171071907)

[6.3 Security vulnerabilities are identified and addressed. 11](#_Toc171071908)

[6.4 Public-facing web applications are protected against attacks. 11](#_Toc171071909)

[6.5 Changes to all system components are managed securely. 11](#_Toc171071910)

[Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know 13](#_Toc171071911)

[Purpose 13](#_Toc171071912)

[Scope 13](#_Toc171071913)

[7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. 13](#_Toc171071914)

[7.2 Access to system components and data is appropriately defined and assigned. 13](#_Toc171071915)

[7.3 Access to system components and data is managed via an access control system(s). 13](#_Toc171071916)

[Requirement 8: Identify Users and Authenticate Access to System Components 14](#_Toc171071917)

[Purpose 14](#_Toc171071918)

[Scope 14](#_Toc171071919)

[8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood. 14](#_Toc171071920)

[8.2 User identification and related accounts for users and administrators are strictly managed throughout an account’s lifecycle. 14](#_Toc171071921)

[8.3 Strong authentication for users and administrators is established and managed. 14](#_Toc171071922)

[8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE. 14](#_Toc171071923)

[8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse. 15](#_Toc171071924)

[8.6 Use of application and system accounts and associated authentication factors is strictly managed. 15](#_Toc171071925)

[Requirement 9: Restrict Physical Access to Cardholder Data 16](#_Toc171071926)

[Purpose 16](#_Toc171071927)

[Scope 16](#_Toc171071928)

[9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood. 16](#_Toc171071929)

[9.2 Physical access controls manage entry into facilities and systems containing cardholder data. 16](#_Toc171071930)

[9.3 Physical access for personnel and visitors is authorized and managed. 16](#_Toc171071931)

[9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed. 16](#_Toc171071932)

[9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution. 16](#_Toc171071933)

[Requirement 10: Log and Monitor All Access to System Components and Cardholder Data 18](#_Toc171071934)

[Purpose 18](#_Toc171071935)

[Scope 18](#_Toc171071936)

[10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood. 18](#_Toc171071937)

[10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. 18](#_Toc171071938)

[10.3 Audit logs are protected from destruction and unauthorized modifications. 18](#_Toc171071939)

[10.4 Audit logs are reviewed to identify anomalies or suspicious activity. 18](#_Toc171071940)

[10.5 Audit log history is retained and available for analysis. 19](#_Toc171071941)

[10.6 Time-synchronization mechanisms support consistent time settings across all systems. 19](#_Toc171071942)

[10.7 Failures of critical security control systems are detected, reported, and responded to promptly. 19](#_Toc171071943)

[Requirement 11: Test Security of Systems and Networks Regularly 20](#_Toc171071944)

[Purpose 20](#_Toc171071945)

[Scope 20](#_Toc171071946)

[11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood. 20](#_Toc171071947)

[11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed. 20](#_Toc171071948)

[11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed. 20](#_Toc171071949)

[11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected. 20](#_Toc171071950)

[11.5 Network intrusions and unexpected file changes are detected and responded to. 21](#_Toc171071951)

[11.6 Unauthorized changes on payment pages are detected and responded to. 21](#_Toc171071952)

[Requirement 12: Support Information Security with Organizational Policies and Programs 22](#_Toc171071953)

[Purpose 22](#_Toc171071954)

[Scope 22](#_Toc171071955)

[12.1 A comprehensive information security policy that governs and provides direction for protection of the entity’s information assets is known and current. 22](#_Toc171071956)

[12.2 Acceptable use policies for end-user technologies are defined and implemented. 22](#_Toc171071957)

[12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed. 22](#_Toc171071958)

[12.4 PCI DSS compliance is managed. 22](#_Toc171071959)

[12.5 PCI DSS scope is documented and validated. 23](#_Toc171071960)

[12.6 Security awareness education is an ongoing activity. 23](#_Toc171071961)

[12.7 Personnel are screened to reduce risks from insider threats. 23](#_Toc171071962)

[12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed. 23](#_Toc171071963)

[12.9 Third-party service providers (TPSPs) support their customers’ PCI DSS compliance. 23](#_Toc171071964)

[12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately. 23](#_Toc171071965)

|  |  |
| --- | --- |
| PCI Data Security Standard Overview | |
| Build and Maintain a Secure Network and Systems | 1. Install and Maintain Network Security Controls 2. Apply Secure Configurations to all system components |
| Protect Account Data | 1. Protect Stored Account Data 2. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks |
| Maintain a Vulnerability Management Program | 1. Protect All Systems and Networks from Malicious Software 2. Develop and Maintain Secure Systems and Software |
| Implement Strong Access Control Measures | 1. Restrict Access to System Components and Cardholder Data by Business Need to Know 2. Identify Users and Authenticate Access to System Components 3. Restrict Physical Access to Cardholder Data |
| Regularly Monitor and Test Networks | 1. Log and Monitor All Access to System Components and Cardholder Data 2. Test Security of Systems and Networks Regularly. |
| Maintain an Information Security Policy | 1. Support Information Security with Organizational Polices and Programs. |

PCI Data Security Standard Policy

Requirement 1: Install and Maintain Network Security Controls

Purpose

To ensure the protection of cardholder data by implementing and maintaining effective network security controls. This policy aims to prevent unauthorized access and secure the cardholder data environment (CDE) through clear and understandable processes for all relevant personnel at [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear steps and tools are used to set up and take care of network security measures, ensuring everyone knows what to do. This involves using documented procedures and training for the team and employing automated deployment tools.

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

The security tools and settings that protect the network are properly set up and regularly checked to keep them working well. This includes configuring firewalls, intrusion detection systems, and regularly updating these systems to protect against new threats.

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

Strict rules control who can access the network area where cardholder data is stored, ensuring only authorized people can get in or out. This means using access control lists (ACLs), setting up VPNs, and requiring strong authentication methods like multi-factor authentication (MFA).

1.4 Network connections between trusted and untrusted networks are controlled.

There are safeguards to manage and monitor the connections between safe, trusted networks and less secure, untrusted ones. This includes using firewalls to filter traffic, implementing demilitarized zones (DMZs), and employing network segmentation to separate different network areas.

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

Measures are in place to reduce the dangers posed by devices that can connect to both insecure networks and the secure area where cardholder data is kept. This involves using network access control (NAC) solutions, enforcing security policies on connected devices, and regularly monitoring device activity.

Requirement 2: Apply Secure Configurations to All System Components

Purpose

To ensure all system components are securely configured and managed to protect cardholder data. This policy aims to prevent vulnerabilities and ensure the secure operation of all systems within [Your Organization’s Name], providing clear guidance for all relevant personnel.

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear guidelines and methods are in place to ensure all parts of the system are set up securely, and everyone understands how to follow them. This means using tools to automatically set up systems correctly, following best practices, and using scripts to ensure everything is done the same way each time.

2.2 System components are configured and managed securely.

All parts of the system are set up and maintained in a way that keeps them safe from threats. This includes regularly updating software, scanning for security weaknesses, and applying fixes quickly using management tools.

2.3 Wireless environments are configured and managed securely.

Wireless networks are set up and looked after in a way that ensures they remain secure. This means using strong passwords and encryption, separating different parts of the network, and watching for unusual activity using monitoring tools.

Requirement 3: Protect Stored Account Data

Purpose

To ensure the protection of stored account data, including cardholder data, through effective security measures. This policy aims to minimize the storage of sensitive information, prevent unauthorized access, and protect data integrity within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are in place to protect stored account data, and everyone knows how to use them. This includes using encryption and access controls to keep data safe.

3.2 Storage of account data is kept to a minimum.

Only the necessary account data is stored, and nothing extra is kept. This means regularly reviewing and deleting unnecessary data.

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

Sensitive data like PINs, card security codes, and passwords are not kept after they are used to verify transactions. This involves configuring systems to automatically delete this data after use.

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

Viewing and copying the full card number (PAN) is tightly controlled to prevent unauthorized access. This includes masking PANs in displays and logs, and using strict access controls.

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

The card number (PAN) is protected no matter where it is kept. This means using encryption, tokenization, or hashing to make sure the PAN is unreadable to unauthorized users.

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

The keys used for encrypting account data are kept safe. This involves using hardware security modules (HSMs) or other secure key management solutions to store and manage the keys.

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.

Clear rules and methods are in place for managing cryptographic keys at all stages, from creation to destruction. This includes procedures for generating, distributing, storing, rotating, and retiring keys securely.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over, Open, Public Networks

Purpose

To ensure the protection of cardholder data during transmission over open, public networks by using strong cryptography. This policy aims to prevent unauthorized interception and access to sensitive information, ensuring secure communication within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are used to protect cardholder data when it is sent over the internet or other public networks, and everyone knows how to follow these methods. This includes using encryption protocols like TLS (Transport Layer Security) to secure data during transmission.

4.2 PAN is protected with strong cryptography during transmission

The card number (PAN: Primary Account Number) is encrypted when it is sent over networks to keep it safe from unauthorized access. This means using strong encryption methods like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) to ensure the data remains secure while being transmitted.

Requirement 5: Protect All Systems and Networks from Malicious Software

Purpose

To protect all systems and networks from malicious software (malware) by implementing effective prevention, detection, and response mechanisms. This policy aims to safeguard cardholder data and ensure the integrity and security of all IT assets within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are in place to protect all systems and networks from harmful software, and everyone understands how to use them. This includes using antivirus programs, regular system scans, and keeping software up to date to prevent vulnerabilities.

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

Harmful software is blocked or found and dealt with quickly. This involves using real-time monitoring tools, employing intrusion detection systems, and having response plans ready to remove any detected malware.

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

Tools and methods to fight harmful software are always running, kept up to date, and regularly checked. This means keeping antivirus software updated, running regular scans, and monitoring systems continuously to catch any issues early.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

Tools and methods are in place to protect users from fraudulent attempts to steal personal information through fake emails or websites. This includes using email filtering tools, providing user training on recognizing phishing attempts, and deploying browser security features to block suspicious sites.

Requirement 6: Develop and Maintain Secure Systems and Software

Purpose

To ensure the development and maintenance of secure systems and software, thereby protecting cardholder data from potential vulnerabilities and attacks. This policy aims to guide the secure creation and management of software and systems within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are in place for creating and maintaining secure systems and software, and everyone understands how to use them. This includes following secure coding practices, using code review tools, and adhering to security guidelines throughout the development process.

6.2 Bespoke and custom software are developed securely.

Custom-made software is created with security in mind from the start. This involves performing regular security assessments, using secure coding standards, and incorporating security testing into the development lifecycle.

6.3 Security vulnerabilities are identified and addressed.

Weak points in systems and software are found and fixed promptly. This includes using vulnerability scanning tools, performing regular security audits, and applying patches or updates to address any identified issues.

6.4 Public-facing web applications are protected against attacks.

Web applications that are accessible to the public are safeguarded from potential threats. This means implementing security measures like web application firewalls (WAFs), conducting penetration testing, and using secure coding practices to prevent common attacks such as SQL injection and cross-site scripting (XSS).

6.5 Changes to all system components are managed securely.

Any modifications to system components are handled in a secure manner. This involves using change management processes, maintaining detailed logs of changes, and ensuring that updates are tested in a secure environment before being applied to live systems.

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

Purpose

To restrict access to system components and cardholder data strictly based on business need-to-know principles. This policy aims to protect sensitive information by ensuring that access is granted only to those with legitimate business needs within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are used to limit access to system components and cardholder data only to those who need it for their job. This includes implementing role-based access control (RBAC), ensuring access is granted based on job responsibilities, and regularly reviewing access rights.

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

Permissions for accessing system components and data are clearly set and given out correctly. This involves creating detailed access policies, using identity and access management (IAM) tools, and assigning permissions based on the principle of least privilege.

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

Access to systems and data is controlled through a dedicated access management system. This includes using systems like Active Directory (AD) for managing user access, implementing multi-factor authentication (MFA) for additional security, and regularly monitoring and auditing access logs.

Requirement 8: Identify Users and Authenticate Access to System Components

Purpose

To ensure the identification and authentication of users accessing system components, thereby safeguarding cardholder data. This policy aims to establish strong authentication practices and prevent unauthorized access within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are in place for identifying users and verifying their access to system components, ensuring everyone understands how to follow them. This includes using unique user IDs, strong passwords, and authentication protocols.

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

User and administrator accounts are carefully managed from creation to deletion. This involves regularly reviewing account permissions, disabling inactive accounts, and using automated tools to manage account changes.

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

Secure methods are used to verify the identities of users and administrators. This includes implementing strong password policies, using biometric verification, and employing single sign-on (SSO) systems for secure access.

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

Additional layers of security are used to verify user identities when accessing the cardholder data environment (CDE). This means requiring something the user knows (like a password) and something they have (like a security token) or something they are (like a fingerprint).

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

MFA systems are set up to ensure they cannot be easily bypassed or misused. This involves configuring systems to lock accounts after multiple failed attempts, using secure channels for delivering authentication codes, and regularly updating MFA settings.

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

Application and system accounts are carefully controlled and monitored. This includes limiting the use of shared accounts, regularly rotating authentication keys or passwords, and auditing the use of these accounts to ensure compliance with security policies.

Requirement 9: Restrict Physical Access to Cardholder Data

Purpose

To ensure the protection of cardholder data by restricting physical access to authorized personnel only. This policy aims to prevent unauthorized physical access, tampering, and theft of sensitive information within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are in place to limit who can physically access cardholder data, and everyone understands how to follow them. This includes using security policies, physical barriers, and staff training.

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

Controls are in place to manage who can enter facilities and access systems that contain cardholder data. This involves using key cards, biometric scanners, and security personnel to monitor and control access points.

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

Access for both employees and visitors is carefully controlled and monitored. This means issuing visitor badges, maintaining access logs, and ensuring that only authorized personnel have access to sensitive areas.

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

Any media containing cardholder data, such as paper records or storage devices, is handled securely throughout its lifecycle. This includes using locked storage, secure distribution methods, and properly shredding or destroying media when no longer needed.

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

Devices used for transactions, such as card readers, are protected against tampering and being replaced with fraudulent devices. This involves regularly inspecting devices, using tamper-evident seals, and monitoring for any signs of tampering or replacement.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Purpose

To ensure all access to system components and cardholder data is logged and monitored for security purposes. This policy aims to detect and respond to anomalies, suspicious activities, and security incidents within [Your Organization’s Name].

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are used to log and monitor access to all system components and cardholder data, ensuring everyone understands how to use them. This includes using centralized logging systems and setting up alerts for unusual activity.

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

Logs are set up to help find unusual or suspicious activities and to analyze events after they happen. This involves configuring systems to log detailed access and activity information and using tools to analyze these logs.

10.3 Audit logs are protected from destruction and unauthorized modifications.

Logs are kept safe from being deleted or changed by unauthorized people. This includes using secure storage methods, access controls, and regular backups.

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

Logs are regularly checked to find any unusual or suspicious activities. This involves setting up regular review schedules, using automated tools to flag potential issues, and having staff trained to interpret the logs.

10.5 Audit log history is retained and available for analysis.

Historical logs are kept and can be accessed for review and analysis when needed. This means having policies for how long logs should be kept and ensuring they are stored in a way that makes them easily retrievable.

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

Systems are synchronized to the same time to ensure logs have accurate timestamps. This includes using Network Time Protocol (NTP) servers to keep all systems' clocks in sync.

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

Any failures in important security systems are quickly found, reported, and fixed. This involves setting up monitoring tools to detect failures, having alerting mechanisms in place, and ensuring there are processes for responding to these alerts promptly.

Requirement 11: Test Security of Systems and Networks Regularly

Purpose

To ensure the security of systems and networks through regular testing and monitoring. This policy aims to identify and address vulnerabilities, prevent unauthorized access, and maintain the integrity of [Your Organization’s Name] systems and networks.

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

Clear methods and tools are used to regularly check the security of systems and networks, ensuring everyone knows how to use them. This includes scheduling regular security assessments, vulnerability scans, and compliance checks.

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

Wireless access points are regularly checked and monitored to ensure they are authorized, and any unauthorized ones are dealt with promptly. This involves using network monitoring tools to detect all access points and employing security measures to block unauthorized ones.

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

Weaknesses in the system, both from outside and inside the organization, are regularly found, ranked by importance, and fixed. This includes running regular vulnerability scans, using patch management systems, and prioritizing fixes based on risk assessments.

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

Regular simulated attacks are carried out to test the defenses of the system, and any found weaknesses are fixed. This involves hiring external security experts to perform penetration tests and ensuring that any discovered vulnerabilities are promptly addressed.

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

Any unauthorized access to the network or unexpected changes to files are quickly identified and dealt with. This means using intrusion detection systems (IDS), file integrity monitoring tools, and having a response plan in place to handle incidents.

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

Changes to payment pages are monitored for unauthorized modifications, and any such changes are addressed immediately. This includes using web application firewalls (WAFs), content monitoring tools, and having processes for rapid response to any detected changes.

Requirement 12: Support Information Security with Organizational Policies and Programs

Purpose

To support the protection of information assets through comprehensive organizational policies and programs. This policy ensures that information security is maintained across all levels of [Your Organization’s Name] by providing clear guidelines and continuous education to all relevant personnel.

Scope

Applies to all employees, contractors, business associates, and outsourced providers of [Your Organization’s Name] who handle cardholder data.

*Organization shall:*

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

A detailed security policy that guides how to protect the organization’s information is well-known and up to date. This includes regular reviews and updates of the policy to reflect new security threats and business practices.

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

Rules for how employees can use company technology are clearly defined and put into practice. This involves setting guidelines for using computers, smartphones, and the internet, and ensuring employees understand and follow these rules.

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

Potential threats to the area where cardholder data is stored are systematically identified, assessed, and mitigated. This includes conducting risk assessments, documenting risks, and implementing measures to reduce these risks.

12.4 PCI DSS compliance is managed.

Ensuring that the organization follows PCI DSS (Payment Card Industry Data Security Standard) requirements is actively managed. This involves regular compliance checks, maintaining required documentation, and addressing any non-compliance issues promptly.

12.5 PCI DSS scope is documented and validated.

The boundaries of what is covered under PCI DSS requirements are clearly documented and regularly checked to ensure accuracy. This means identifying all systems and processes that handle cardholder data and ensuring they meet PCI DSS standards.

12.6 Security awareness education is an ongoing activity.

Training and education about security practices are provided regularly to keep all employees informed. This includes holding security awareness sessions, sending out reminders about best practices, and updating training materials as needed.

12.7 Personnel are screened to reduce risks from insider threats.

Employees undergo background checks and other screening processes to minimize the risk of insider threats. This involves verifying the qualifications and backgrounds of new hires and conducting periodic re-screening of existing employees.

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

Risks related to using third-party service providers are identified and controlled. This includes assessing the security practices of TPSPs, ensuring they comply with security requirements, and monitoring their activities.

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

Third-party service providers are required to assist their clients in meeting PCI DSS standards. This involves ensuring that TPSPs understand their role in PCI DSS compliance and provide necessary documentation and support.

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

Any suspected or confirmed security breaches that could affect the cardholder data environment are addressed right away. This includes having an incident response plan in place, training staff on how to respond, and ensuring incidents are reported and handled promptly.