PCI Policy

All In-scope PCI DSS Requirements

**Version:** 0.1

**Date:** [Date]

**Reference:**

**Status:** Draft

**Security Classification:** Internal

Contents

[1 Policy Statement 3](#_Toc134705003)

[2 Review and Update of this Policy 3](#_Toc134705004)

[3 Purpose 3](#_Toc134705005)

[4 Scope 3](#_Toc134705006)

[4.1 Networks in Scope: 3](#_Toc134705007)

[5 Policy Requirements 4](#_Toc134705008)

[5.1 PCI DSS Requirement 1 - Not in scope for [Company] 4](#_Toc134705009)

[5.2 PCI DSS Requirement 2 – Apply Secure Configurations to all Server components 5](#_Toc134705010)

[5.2.1 Vendor / Support Default Accounts 5](#_Toc134705011)

[5.3 PCI DSS Requirement 3 - Protect Stored Cardholder Data 6](#_Toc134705012)

[5.3.1 Requirement 3 Policies 6](#_Toc134705013)

[5.3.2 Data Storage Restrictions 6](#_Toc134705014)

[5.4 PCI DSS Requirement 4 - Not in scope for [Company] 7](#_Toc134705015)

[5.5 PCI DSS Requirement 5 - Not in scope for [Company] 8](#_Toc134705016)

[5.6 PCI DSS Requirement 6 - Develop and maintain secure systems and applications 9](#_Toc134705017)

[5.6.1 System Vulnerabilities 9](#_Toc134705018)

[5.6.2 System Updates 9](#_Toc134705019)

[5.6.3 Payment Scripts 9](#_Toc134705020)

[5.7 PCI DSS Requirement 7 - Not in scope for [Company] 10](#_Toc134705021)

[5.8 PCI DSS Requirement 8 - Identify and authenticate access to system components 11](#_Toc134705022)

[5.8.1 Issuing of Accounts 11](#_Toc134705023)

[5.8.2 Termination / Suspension of Employment 11](#_Toc134705024)

[5.8.3 Password / Session Lockout and Resetting 11](#_Toc134705025)

[5.9 PCI DSS Requirement 9 - Restrict physical access to cardholder data 13](#_Toc134705026)

[5.9.1 Security Perimeters 13](#_Toc134705027)

[5.9.2 Backup Security and Physical Media 13](#_Toc134705028)

[5.9.3 Distribution 13](#_Toc134705029)

[5.9.4 Secure Disposal of Physical Media 13](#_Toc134705030)

[5.10 PCI DSS Requirement 10 - Not in scope for [Company] 14](#_Toc134705031)

[5.11 PCI DSS Requirement 11 - Regularly test security systems and processes 15](#_Toc134705032)

[5.11.1 Vulnerability Assessments 15](#_Toc134705033)

[5.11.2 Mobile & Devices 15](#_Toc134705034)

[5.12 PCI DSS Requirement 12 - Maintain an Information Security Policy 16](#_Toc134705035)

[5.12.1 Service Providers 16](#_Toc134705036)

[5.12.2 System Breach 16](#_Toc134705037)

[6 Policy Mapping 17](#_Toc134705038)

[7 Definitions and References 18](#_Toc134705039)

[7.1 Definitions 18](#_Toc134705040)

|  |  |  |
| --- | --- | --- |
| Version Number | Description | Author |
| V0.1 | Initial Policy Creation | [Author] |

# Policy Statement

This [Company] Security Policy:

* Sets out high level requirements for the management of security at [Company] in relation to the storage, processing and transmission of credit card data and personal data
* Defines the security policy for the business.
* Applies to all credit card processing operations for the business.
* Applies to all data protection operations for the business.

# Review and Update of this Policy

This policy and associated company policies shall be reviewed at least annually by the Security Review Team to ensure that:

* The business meets its compliance obligations to the Payment Card Industry Data Security Standard (PCI DSS)
* The business meets its compliance obligations to the UK Data Protection law and General Data Protection Regulations
* It maintains its relevance to the business’ current and planned credit card processing operations.
* It maintains its relevance to the business’ current and planned data retention and protection obligations.

Operations team members will undertake the technical review of this policy and associated company policies.

# Purpose

This document details guidelines and procedures for members of staff and any third parties that intend to perform network operations within the [Company]’s data environments.

# Scope

This document provides instruction on maintaining ’s cardholder data environment to Payment Card Industry standards.

It is restricted to those employees, companies or contractors that process, store or transmit credit card data on behalf of or have access to such systems.

## Networks in Scope:

| **Network Name** | **Description** |
| --- | --- |
| [Network] | [Desc] |

# Policy Requirements

## PCI DSS Requirement 1 - Not in scope for

## PCI DSS Requirement 2 – Apply Secure Configurations to all Server components.

### Vendor / Support Default Accounts

User accounts issued to product vendors or for support purposes shall only be activated when required for support requirements and disabled immediately when no longer required. Vendor accounts for remote access should be monitored while being used, and access should be restricted to the time period needed.

## 

## PCI DSS Requirement 3 - Protect Stored Cardholder Data

### Requirement 3 Policies

All security policies and operational procedures for Requirement 3 must be documented, kept up to date, actively used, and known to all affected parties. Regular reviews and training should be conducted to ensure compliance, and periodic assessments should be performed to identify and address any gaps or weaknesses.

### Data Storage Restrictions

The following sensitive authentication data shall not be stored by [Company] on any medium whatsoever under any circumstances:

* Track Data
* Card Validation Code (CVV2, CVC2, CID, CAV2) (except for pre-authorisation transactions)
* Encrypted PIN block
* PIN or PIN Verification Values

For all instances where sensitive data is received and deleted as part of transaction processing:

* must identify the document, defining the processes for securely deleting sensitive data.
* must verify the processes used to render data unrecoverable are tested and how sensitive data is confirmed as unrecoverable.

The company must also

## PCI DSS Requirement 4 - Not in scope for

## PCI DSS Requirement 5 - Not in scope for

## PCI DSS Requirement 6 - Develop and maintain secure systems and applications.

### System Vulnerabilities

must establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

### System Updates

shall maintain a list (or have the capability to generate one) of patches installed on every server.

Software updates shall be applied to internal systems on an on-going basis to ensure the systems are hardened against developing security threats.

Software and security patches for critical infrastructure must be installed within 30 days of release and lower priority infrastructure within three months.

shall schedule software updates to systems to occur prior to the commencement of the business day, at a time in order to minimise disruption.

Updates destined for live systems shall be tested beforehand on test systems to determine whether or not they shall cause any disruption to front line, client facing systems.

All updates shall require the person completing the update to complete the Change Control entry and obtain signoffs.

### Payment Scripts

All scripts utilized by [Company] for payment processing must undergo authorization, ensuring their suitability and compliance with established standards. The authorization process involves a thorough review and approval by the appropriate stakeholders, such as the IT department, security team, and management.

A robust method must be implemented to verify the authenticity and integrity of all payment processing scripts. This verification process should include measures to ensure that the scripts have not been tampered with or modified without proper authorization. Suitable methods for script verification may include digital signatures, version control systems, cryptographic checksums, or other industry-standard mechanisms.

[Company] is responsible for maintaining the integrity of all payment processing scripts throughout their lifecycle. This involves implementing controls to prevent unauthorized access, modification, or deletion of scripts. Additionally, appropriate change management practices should be followed to track and document any modifications made to the scripts.

Regular maintenance of payment processing scripts is crucial to ensure their effectiveness, efficiency, and security. Maintenance activities may include patching known vulnerabilities, updating libraries or dependencies, optimizing performance, and addressing any issues or bugs identified during the course of operation. A documented schedule for script maintenance should be established to ensure timely updates and to minimize any potential disruptions to payment processing operations.

[Company] must provide written justification for the necessity of each payment processing script used. This justification should outline the specific purpose of the script and explain why it is essential for payment processing operations. The written justifications serve as a reference for auditing, compliance, and management purposes, ensuring transparency and accountability in the use of payment processing scripts.

## PCI DSS Requirement 7 - Not in scope for

## 

## PCI DSS Requirement 8 - Identify and authenticate access to system components.

### Issuing of Accounts

The **[Company] Operations Team** or nominated deputies are responsible for authorising and ensuring that access is formally assigned and that accounts are issued, deleted or modified. Each employee shall be issued a unique user account and password, issued for the individual’s own use only. The account must be configured to require the password to be changed immediately after first use.

Upon commencement of employment, a new user account shall be activated by the **[Company]** **Operations Team,** and a password set in accordance with password policy, or issuing of a token device or use of biometrics, as is relevant.

Under **no** circumstances shall group, generic or shared accounts be issued to **any** user(s) even if requested. If any group, generic or shared accounts are found they should be either disabled or removed.

The issuing of accounts must follow these guidelines for all critical technologies used to access the cardholder data environment, including remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data / digital assistants (PDAs), e-mail and Internet usage. shall ensure that all access to cardholder data is controlled and monitored.

The creation of accounts is on the basis of the personnel’s job classification and function.

### Termination / Suspension of Employment

The **[Company] Operations Team** shall be informed as soon as a person’s employment is terminated without exception and be required to suspend the former employee’s access credentials immediately.

Should a member of staff be suspended as a result of a disciplinary procedure, the **[Company] Operations Team** should be informed and access to electronic resources shall be suspended immediately until the procedure is completed.

### Password / Session Lockout and Resetting

shall use strong cryptography, to render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

Applications and Network infrastructure shall lock access to an account after six (6) failed login attempts.

* Locked accounts will auto-unlock after 60 minutes. Unlocking / resetting passwords within this time shall require the user to contact the Operations Team in person to verify the user is legitimate. Where this is not possible, shall verify the user’s identity before performing password resets, via PGP encrypted e-mail, Video Conferencing/Skype, direct phone contact.
* The account will remain locked out for 30 minutes or until the administrator unlocks the account.
* Users must change their passwords upon initial login or when provided with temporary credentials.
* Passwords must have a minimum length of 12 characters, unless unsupported systems restrict the maximum length to 8 characters.
* Passwords must include a combination of both numeric and alphabetic characters to enhance complexity and security.
* Users are prohibited from reusing any of their previous four passwords. This measure ensures that passwords remain unique and strengthens overall security.
* Passwords must be refreshed every 90 days. Users are required to change their passwords periodically to maintain account security and minimize the risk of unauthorized access.
* Remote Login sessions shall time-out after being idle for 15 minutes and require the user to re-login.
* Local login sessions shall lock after 5 minutes to prevent unauthorised access to user data.
* The User shall be required to input his or her password in order to continue.

must incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

## PCI DSS Requirement 9 - Restrict physical access to cardholder data.

### Security Perimeters

All buildings and entry points must be of substantial structure and able to withstand a reasonable forced entry attack so as not to undermine the security controls applied to the entry point.

requires that cardholder data processing areas only have physical entry points from the internal perimeter. This applies to facilities managed by or any third-party supplier.

### Backup Security and Physical Media

Wherever possible backup and storage of personal data or cardholder data shall be within the same environment as the originating data. By following this approach, backed up data is subject to the physical and other security controls already present in the originating environment.

Nevertheless, this policy describes the policy should hard copy or backup media be used.

#### Cloud Data Centres

Personal data is backed up at regular intervals within the cloud environment.

### Distribution

Maintain strict control over the internal or external distribution of any kind of media, including the following.

* Classify media so the sensitivity of the data can be determined.
* Send the media by secured courier or other delivery method that can be accurately tracked.
* Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals)

### Secure Disposal of Physical Media

When no longer required for backup purposes data must be disposed of in a secure manner, as follows:

* Data in digital format (hard disk, backup tapes etc.) shall be disposed of using secure delete facilities (e.g., write-rewrite multiple times) prior to the disposal of the hardware.
* Physical media shall be physically destroyed prior to disposal to ensure no data can be recovered.

## PCI DSS Requirement 10 - Not in scope for

## PCI DSS Requirement 11 - Regularly test security systems and processes.

### Vulnerability Assessments

External vulnerability scans are conducted once every three months by a PCI Approved Scanning Vendor (ASV) to proactively identify and address security weaknesses. Scans utilize industry-standard tools and techniques to comprehensively assess external-facing systems and networks. Identified vulnerabilities are promptly documented and prioritized based on their severity, with a focus on resolving those with a CVSS score of 4.0 or higher.

Additionally, scans are performed after significant changes to assess the security posture of affected systems or networks. Qualified personnel conduct these scans, identifying priority vulnerabilities with a CVSS score of 4.0 or higher. Prompt measures are taken to mitigate risks associated with these vulnerabilities.

To ensure integrity and impartiality, [Company] maintains organizational independence in the assessment process, except for cases involving Qualified Security Assessors (QSA) or Approved Scanning Vendors (ASV) with direct affiliations.

Rescans are performed as needed to verify the effectiveness of remediation efforts, providing assurance that vulnerabilities have been adequately addressed and systems remain secure.

### Mobile & Devices

A log of all mobile and wireless network devices shall be maintained. These logs shall detail which staff member is responsible for the device, when it was taken and when it is returned.

must protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.

Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

Maintain an up-to-date list of devices. The list should include the following:

* Make, model of device.
* Location of device (for example, the address of the site or facility where the device is located).
* Device serial number or other method of unique identification

## PCI DSS Requirement 12 - Maintain an Information Security Policy

### Service Providers

shall maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

* Maintain list of service providers
* Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE.
* Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
* Maintain a program to monitor service providers’ PCI DSS compliance status at least annually.
* Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

Service providers must acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.

If is a service provider, quarterly reviews must be performed to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes.

* Daily log reviews
* Firewall rule-set reviews
* Applying configuration standards to new systems
* Responding to security alerts
* Change management processes.

As well as maintaining documentation of quarterly review process to include.

* Documenting results of the reviews
* Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

### System Breach

must implement an incident response plan. Be prepared to respond immediately to a system breach. This incident response plan must be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

* Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum.
* Specific incident response procedures.
* Business recovery and continuity procedures.
* Data back-up processes.
* Analysis of legal requirements for reporting compromises.
* Coverage and responses of all critical system components.
* Reference or inclusion of incident response procedures from the payment brands

must.

* Test the plan at least annually.
* Designate specific personnel to be available on a 24/7 basis to respond to alerts.
* Provide appropriate training to staff with security breach response responsibilities.
* Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.
* Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

# Policy Mapping

The requirements are mapped as follows.

|  |  |  |
| --- | --- | --- |
| PCI Requirement Number | Description | Page Reference |
| 2.2.2 | Vender Default Accounts | 5.2.1 |
| 3.1.1 | Requirement 3 Policies | 5.3.1 |
| 3.2.1 | Data Storage Requirements | 5.3.2 |
| 6.3.1 | System Vulnerabilities | 5.6.1 |
| 6.3.3 | System Updates | 5.6.2 |
| 6.4.3 | Payment Page Scripts | 5.6.3 |
| 8.2.1 | Account IDs | 5.8.1 |
| 8.2.2 | Shared Accounts | 5.8.1 |
| 8.2.3 | Termination of Accounts | 5.8.2 |
| 8.3.1 | Authentication Methods | 5.8.3 |
| 8.3.5 | Password Reset | 5.8.3 |
| 8.3.6 | Password Complexity | 5.8.3 |
| 8.3.7 | Password History | 5.8.3 |
| 8.3.9 | Password Expiry | 5.8.3 |
| 9.4.1 | Cardholder Data Secured | 5.9.1 |
| 9.4.1.1 | Backups | 5.9.2/5.9.2.1 |
| 9.4.3 | Distribution of Data | 5.9.3 |
| 9.4.4 | Management Approval of Distribution | 5.9.3 |
| 9.4.6 | Disposal of Physical Data | 5.9.4 |
| 11.3.2 | External Vulnerability Scans Schedule | 5.11.1 |
| 11.3.2.1 | External Vulnerability Scans after significant change | 5.11.1 |
| 11.6.1 | Anti-Tamper/Change | 5.11.2 |
| 12.8.1 | List of Third-Party Providers (TPSPs) | 5.12.1 |
| 12.8.2 | Written agreement with TPSPs | 5.12.1 |
| 12.8.3 | Engaging with TPSPs | 5.12.1 |
| 12.8.4 | Monitoring TPSPs Compliance | 5.12.1 |
| 12.8.5 | Requirement tracking | 5.12.1 |
| 12.10.1 | Incident Response Plan | 5.12.2 |

# Definitions and References

## Definitions

* **IS:** Information Security
* **Payment Card Industry Data Security Standard (PCI DSS):** Currently referenced directly from The PCI Security Standards Council’s online resource at <https://www.pcisecuritystandards.org>
* **QSA:** Qualified Security Assessor. A third-party assessor that conducts onsite PCI audits for Service Providers and Merchants. The QSA is certified annually by The PCI Security Standards Council
* **ASV:** Approved Scanning Vendor. A third-party assessor that conducts quarterly PCI scans against the external card processing environment. The ASV is certified annually by The PCI Security Standards Council
* **Schemes:** Credit card associated companies that include Visa, MasterCard, Amex, JCB, Diners
* **Merchant:** For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and /or services. Note that a merchant that accepts payment cards as payment for goods and /or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
* **Service Provider:** Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.
* **Acquirer:** Bankcard association member that initiates and maintains relationships with merchants that accept payment cards
* **Cardholder Data:** Full magnetic stripe of the PAN plus any of the following:
* Cardholder name
* Expiration date
* Service Code
* **Cardholder Data Environment:** Area of computer system network that processes cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage or transmission.