POL00362919

IT Security

PCI DSS Compliance Guideline

Version – V2.9

POL00362919

POL00362919

1. Overview

1.1 Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to enhance the security of payment account data. Created by Visa®, Mastercard®, JCB®, Discover® and American Express® it is made up of 12 requirements designed to secure business systems that store, process or transmit card holder data.

1.2 Purpose

The Post Office PCI Guideline is designed to understand how PCI SSC can help to protect Post Office's customer payment card transaction (Store, Process or Transmit cardholder data) environment and how to apply it.

There are three ongoing steps for adhering to the PCI DSS:

Assess — identifying all locations of cardholder data, taking an inventory of your IT assets and business processes for payment card processing and analysing them for vulnerabilities that could expose cardholder data.

Repair — fixing identified vulnerabilities, securely removing any unnecessary cardholder data storage, and implementing secure business processes.

Report — documenting assessment and remediation details, and submitting compliance reports to the acquiring bank and card brands you do business with (or other requesting entity if you're a service provider).

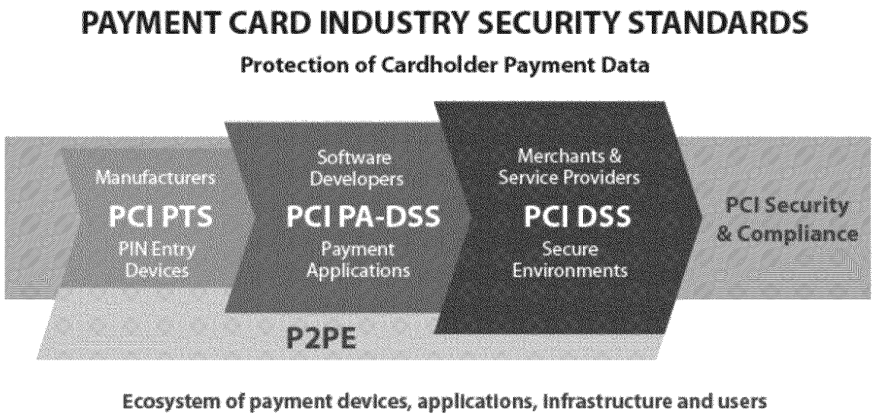
1.3 Application

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or **connected** to cardholder data. If you accept or process payment cards, PCI DSS applies to you.

1.4 PCI Requirements

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions.

POL00362919



PCI Security Standards Include:

1.4.1 PIN Transaction Security (PTS) Requirements

The PCI PTS is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The PTS standards include PIN Security Requirements, Point of Interaction (POI) Modular Security Requirements.

Hardware Security Module (HSM) Security Requirements. The device requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Financial institutions, processors, merchants and service providers should only use devices or components that are tested and approved by the PCI SSC.

1.4.2 Software Security Framework (SSF)

The SSF is for software vendors and others who develop payment applications that store, process, or transmit cardholder data and/or sensitive authentication data as part of authorisation or settlement, when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants to use payment applications that are tested and approved by the PCI SSC.

1.4.3 PCI Point-to-Point Encryption Standard (P2PE)

This Point-to-Point Encryption (P2PE) standard provides a comprehensive set of security requirements for P2PE solution providers to validate their P2PE solutions, and may help reduce the PCI DSS scope of merchants using such solutions. P2PE is a cross-functional program that results in validated solutions incorporating the PTS Standards, PA-DSS, PCI DSS, and the PCI PIN Security Standard.

1.4.4 PCI Token Service Provider Security Requirements

The Token Service Provider (TSP) Security Requirements are intended for Token Service Providers that generate and issue EMV Payment Tokens, as defined under the EMV® Payment Tokenisation Specification Technical Framework.

POL00362919

2 Policy Framework

2.1 Policy Framework

This guideline document is part of the IT Security Policy set. These form the baseline to provide Cyber Security and Information Assurance (CSIA) protection for the Post Office.

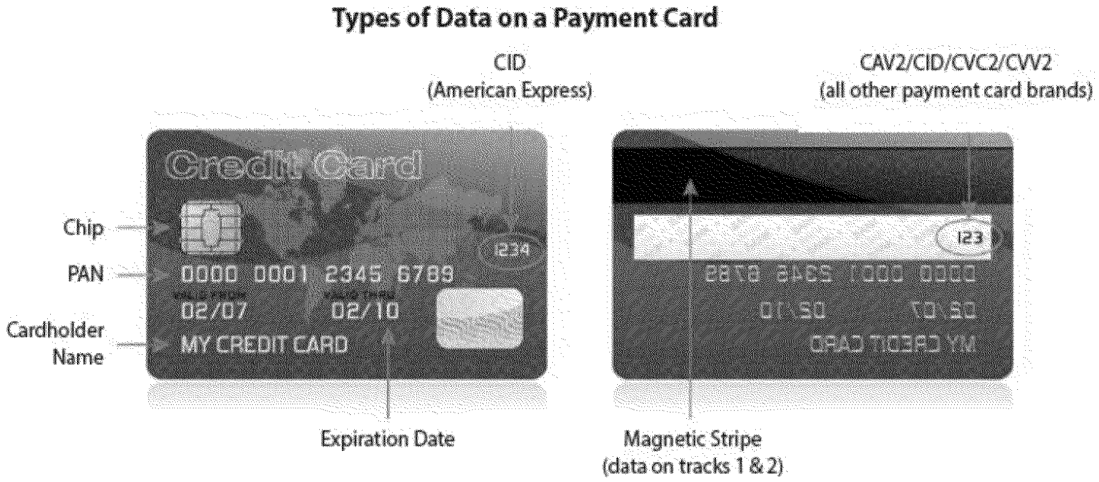
2.2 Who must comply?

Compliance with the IT Security Policy set is mandatory for all Post Office employees and applies wherever in the world Post Offices business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to Post Offices Policies and standards or have their own equivalent policies and standards in place.

POL00362919

3 Security Controls and Processes for PCI DSS Requirements

The goal of this Post Office guideline is to protect cardholder data and sensitive authentication data wherever (Online, Branch, and Mobile Application) it is stored, processed or transmitted. The security controls and processes required by PCI DSS are vital for protecting all payment card account data, including the PAN – the primary account number printed on the front of a payment card. Merchants, service providers, and other entities involved with payment card processing must never store sensitive authentication data after authorisation. This includes the 3- or 4- digit security code printed on the front or back of a card, the data stored on a card's magnetic stripe or chip (also called "Full Track Data") – and personal identification numbers (PIN) entered by the cardholder.



3.1.1 Guideline for Cardholder Data Elements

	Data Element	Storage Permitted	Masking	Render Stored Data Unreadable
Cardholder Data	Primary Account Number (PAN)	Yes (Only truncated). Cardholder data store only Post Office AWS CDE.	Display/ Print mask (e.g. first 6 and last 4 or last 4 digits) PAN.	Yes (Cardholder data store only Post Office AWS CDE)
	Cardholder Name	Yes	No	No
	Service Code	Yes	No	No
	Expiration Date	Yes	No	No
Sensitive Authentication Data	Full Track Data	No	N/A	Must not store
	CAV2/CVC2/CVV 2/CID	No	N/A	Must not store
	PIN/PIN Block	No	N/A	Must not store

POL00362919

The standard specifies 12 requirements which are organised into six control objectives relating to the storage, transmission and processing of cardholder data.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

3.1.2 Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

- Firewalls control the transmission of data between a Post Office's trusted internal networks and untrusted external networks, as well as traffic between sensitive areas of the internal networks themselves. Requirement 1 of the PCI DSS requires systems to use firewalls to prevent unauthorised access. Where other system components provide the functionality of a firewall, they must also be included in the scope and assessment of this requirement.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- The easiest way for a hacker to access your internal network is to try default passwords or exploits based on default system software settings in your payment card infrastructure. Far too often, organisation do not change default passwords or settings upon deployment. Default passwords and settings for most network devices are widely known. This information, combined with hacker tools that show what devices are on your network can make unauthorized entry a simple task – if you have failed to change the defaults.

POL00362919

3.1.3 Protect Cardholder Data

Requirement 3: Protect stored cardholder data

- The storage of cardholder data must be kept to a minimum, and appropriate data retention and disposal policies, procedures and processes must be implemented. When data is stored, it must be stored securely. Encryption, truncation, masking and hashing are critical components of cardholder data protection. Without access to the proper cryptographic keys, encrypted data will be unreadable and unusable by criminal hackers, even if they manage to circumvent other security controls. Cryptographic keys must therefore be stored securely and access restricted to the fewest custodians necessary. Other data protection methods must also be considered
  Sensitive data – such as the full contents of the chip or magnetic strip, the CVN (card verification number) or the PIN (personal identification number) – must not store.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

- Strong cryptography and security protocols (e.g. TLS, IPSec, SSH, etc.) should be used to safeguard sensitive cardholder data during transmission over open, public networks that could easily be accessed by malicious individuals.
  Industry best practices must be followed to implement strong encryption for authentication and transmission. Security policies and procedures for encrypting the transmission of cardholder data must be documented and made known to all affected parties.
  Examples of open, public networks include the Internet, wireless technologies (e.g. Bluetooth), GPRS (general packet radio service) and satellite communications.

3.1.4 Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

- Antivirus software capable of detecting, removing and protecting against all known types of malware (e.g. viruses, worms and Trojans) must be used on all systems commonly affected by malware to protect them from threats. For systems not commonly affected by malware, evolving malware threats should be periodically evaluated to determine if antivirus software is needed. Antivirus mechanisms must be maintained and kept actively running and should only be disabled if formally authorised for a specific purpose.

Requirement 6: Develop and maintain secure systems and applications

- Many security vulnerabilities are fixed by patches issued by software vendors. Organisations should establish a process to identify security vulnerabilities and rank them according to their level of risk. Relevant security patches should be installed within a month of their release to protect against cardholder data compromise. All software applications, developed internally or externally, should be developed securely in accordance with the PCI DSS. They should also be based on industry standards and/or best practices, and incorporate information security throughout their entire development lifecycle.

POL00362919

3.1.5 Implement Strong Access Control Measures

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

- Exploiting authorised accounts and abusing user privileges is one of the easiest ways for criminal hackers to gain access to a system. It is also one of the most difficult types of attack to detect. Documented systems and processes should therefore be put in place to limit access rights to critical data. Access control systems should deny all access by default, and access should be granted on a need-to-know basis and according to the clearly defined job responsibilities of authorised personnel. 'Need to know' is defined in the PCI DSS as "when access rights are granted to only the least amount of data and privileges needed to perform a job".

Requirement 8: Identify and authenticate access to system components

- The ability to identify individual users not only ensures that system access is limited to those with the proper authorisation, it also establishes an audit trail that can be analysed following an incident. Documented policies and procedures must therefore be implemented to ensure proper user identification management for non-consumer users and administrators on all system components. All users must be assigned a unique ID, which must be managed according to specific guidelines. Controlled user authentication management (e.g. the use of passwords, smart cards or biometrics) should also be implemented and, as three-quarters of all network intrusions exploit weak or stolen passwords, 2FA (two-factor authentication) must be used for remote network access.

Requirement 9: Restrict physical access to cardholder data

- Electronic data breaches are not the only source of data loss; physical access to systems should also be limited and monitored using appropriate controls. Procedures should be implemented to distinguish between on-site personnel and visitors, and physical access to sensitive areas (e.g. server rooms and data centres) should be restricted accordingly. All media should be physically secured, and its storage, access and distribution controlled. Media should be destroyed in specific ways when no longer required. Devices that capture payment card data via direct physical interaction with the card must be protected from tampering and substitution, and should be periodically inspected. An up-to-date list of these devices should be maintained.

3.1.6 Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

- The use of logging mechanisms is critical in preventing, detecting and minimising the impact of data compromise. If system usage is not logged, potential breaches cannot be identified. Secure, controlled audit trails must therefore be implemented that link all access to system components with individual users and log their actions. This includes access to cardholder data, actions taken by individuals with root or administrative privileges, access to audit trails, invalid logical access attempts, use of and changes to identification and authentication mechanisms, the initialising, stopping or pausing of audit logs, and the creation and deletion of system-level objects. An audit trail history should be retained for at least a year, with a minimum of three months' logs immediately available for analysis. Logs and

POL00362919

security events should be regularly reviewed to identify anomalous or suspicious activity.

Requirement 11: Regularly test security systems and processes

- New vulnerabilities are regularly found and exploited, so it is essential that system components, processes and custom software are regularly tested. Documented processes must be implemented to detect and identify all unauthorised wireless access points on a quarterly basis. Internal and external network vulnerability scans must be performed by qualified personnel at least quarterly and after any significant change in the network (e.g. new system component installations, changes in network topology, firewall rule modifications and product upgrades). Intrusion detection/prevention techniques should be used to identify and/or prevent unauthorised network activity, and a change detection mechanism should be employed to perform weekly critical file comparisons, and to alert personnel to unauthorised system modifications.

3.1.7 Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

- To comply with the PCI DSS, Post Office established, published, maintained and disseminate a security policies, which reviewed at least annually and updated according to the changing risk environment.
- Post Office risk assessment process in place to identify threats and vulnerabilities, usage policies for critical technologies must be developed, security responsibilities for all personnel has clearly defined and a formal awareness programme rollout on annual basis.
- Post Office incident response plan help to respond immediately to any data /system breach.

POL00362919

4 Business-As-Usual Processes

To ensure security controls continue to be properly implemented, PCI DSS requirements should be implemented into business-as-usual (BAU) activities as part of an Post Office's overall security strategy. This enables the Post Office to monitor the effectiveness of its security controls on an ongoing basis, and maintain its PCI DSS compliant environment in between PCI DSS assessments. Examples of best practices for how to incorporate PCI DSS into BAU activities include (but are not limited to):

- Monitoring of security controls to ensure they are operating effectively and as intended.
- Ensuring that all failures in security controls are detected and responded to in a timely manner.
- Reviewing changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change to ensure PCI DSS scope is updated and controls are applied as appropriate.
- Changes to Post Office structure (for example, a company merger or acquisition) resulting in a formal review of the impact to PCI DSS scope and requirements.
- Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes.
- Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the entity's security requirements, including PCI DSS, and remediating shortcomings as appropriate.

Entities may also consider implementing separation of duties for their security functions so that security and/or audit functions are separated from operational functions.

4.1 Compensating Controls

A compensating control, also called an alternative controls that known to be more complex and generally more difficult to manage compared to the actual control.

The PCI compensating controls (CCW) is broken into seven sections.

1. Identification of the PCI DSS requirement(s) being compensated.
2. The constraint or business justification for needing the CCW.
3. The original objective of the requirement(s) being compensated.
4. Identification of any additional risks because of the CCW
5. The compensating controls.
6. The procedures your QSA/ISA followed to confirm that the compensating controls are in place and functioning.
7. The procedures followed by your organisation to maintain the compensating controls.

POL00362919

5 Where to go for help

5.1 Additional Policies

This standard is one of a set of policies. The Cyber Security policy document set can be found at:

IRRELEVANT

5.2 How to raise a concern

Any Post Office employee who suspects something is wrong has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by contacting the Service Desk and/or email information.security **GRO**

5.3 PCI DSS Truncation Guideline

Acceptable formats for truncation of primary account numbers (FAQ 1091)

https://www.pcisecuritystandards.org/faqs

5.4 Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact the Office of the CISO via cyber **GRO**

POL00362919

6 Version Control

Date	Version	Updated by	Change Details
30/11/2016	1.0	ISAG	First full version of document
08/08/2017	1.1	IPA & IT Security	Changed to new format and minor editorial changes
15/08/2017	2.0	Head of IPA	Accepted to final version.
21/08/2018	2.1	IPA	Minor editorial changes
05/09/2018	2.2	Head of IPA	Accepted to final version
13/08/2019	2.3	IPA	Changes to new format to be based on controls and not statements. No significant changes to requirements.
06/01/2020	2.4	IPA	Changes to new format according to the PCI DSS requirements.
22/01/2020	2.5	Cyber Security	Updated the guideline information according to the Head of Cyber Security Compliance suggestion.
12/03/2021	2.6	Cyber Security	Approved by Head of Cyber Security Compliance.
21/02/2022	2.7	Cyber Security	Updated the section 3.1.1
23/02/2023	2.8	Cyber Security	Annual Review
01/08/2023	2.9	Cyber Security	Updated the Section 1.4.2 and Requirement 3

6.1 Approval

Standard Owner: Chief Information Security Officer

Standard Author: Syed Naqvi

Approved by CSC: 25/04/2023

Next review: 24/04/2024