Cyber Security Standard

Information Classification Standard

Version – V2.2

1 Overview

1.1 Introduction by the Standard Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office

1.2 Purpose

The purpose of the Information Classification Standard is to ensure that access to Post Office information is proportionate and appropriate and to ensure that it is correct, available when needed and only to those who need it.

1.3 Core Principles

Compliance with this standard will ensure that the following principles are met:

- Mandate the classifications to be used for all Post Office information,
- Compliance with regulatory and legislative requirements for protecting information, and
- Provide guidelines for applying this standard.

1.4 Application

This standard relates to all Post Office information and physical assets whether they are owned directly by Post Office or managed on behalf of Post Office by a third party supplier.

2 Policy Framework

2.1 Policy Framework

This standard forms part of the Cyber and Information Security Policy Set**.** This contains controls that form part of the Information Technology Control Framework (ITCF) governed by the overarching Post Office wide framework.

2.2 Who must comply?

Compliance with this standard 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 this standard or have their own equivalent standard/policy.

3 Minimum Controls

The table below sets out the minimum control standards.

Control Ref	Control	Attestation Guidance
PHT0447	Establish, implement, and maintain an access classification scheme.	Information must be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. Any information that is entrusted to Post Office which it does not take ownership for, must be handled according to the classification applied by the originator. Further details on classifications can be found in Appendix A.
PHT0448	Include restricting access to confidential data or restricted information to a need to know basis in the access classification scheme.	Information must be labelled according to it's classification Data flow diagrams must be created and maintained
PHT0449	Include business security requirements in the access classification scheme.	Procedures for handling assets shall be developed and implemented in accordance with the classification of the data. Interpret and apply security requirements based upon the information classification of the system. Retention Schedules need to be kept current. Sector specialists ensure that the contents reflect current industry advice. Schedules must also be kept current.

Control Ref	Control	Attestation Guidance
PHT0451	Include third party access in the access classification scheme.	Guides must be created and maintained ensure that good practice is used by all colleagues in their usage and management of data they have access to or create

4 Appendix A – Classification and Handling

To best protect Post Office information, measures are required to be provided at every part of an IT ecosystem. All Post Office information must be classified with one of the levels identified in this standard. All Post Office information falls into one of the four classifications listed below in order of increasing sensitivity:

Classification	Definition	Handling
PUBLIC	Any public domain information that can be made available to anyone without exception.	• No restriction on storage or handling.
INTERNAL	Information that can be disclosed to anyone signed to a Post Office contract or a non-disclosure agreement.	• Can be shared with anyone signed to a Post Office contract or a non-disclosure agreement. • Should be locked away at the end of the day.
CONFIDENTIAL	Information that must be distributed in a controlled manner; where the Information Owner requires that the information must be shared only on a 'need to know' basis. Unauthorised disclosure of this information could result in financial or reputational damage.	• Must only be shared with employees, agents and contractors who have a "need to know". • Must be stored in Locked containers, official Post Office IT systems and portable media devices protected with encrypted software (please reference the Remote Access and Portable Device Standard, and the Encryption Standard) • If being discussed by phone, the employee must check that they cannot be overheard. • If being sent by post, it should be by hand, Royal Mail Special Deliver or an approved trusted courier named individual. • If to be sent to an external source, must be sent using a secure transfer mechanism, such as Quatrix. Confidential information must never be sent in the clear text by via e-mail or where only opportunistic TLS is in force. • If encrypted using a password, the password must be sent to the recipient by a different channel than the encrypted file – i.e. Send the file by e-mail, SMS the password. • If storing on a SharePoint site, the Information Owner must ensure that all people who have access are authorised to see the content. Regular

Classification	Definition	Handling
		reviews must be performed to make sure access hasn't been given in error (leavers/movers) • Must not be published to the Internet.
STRICTLY CONFIDENTIAL	Information that must be distributed in a highly controlled manner; where the Information Owner requires that the information is shared only within a known set of individual Information Users. This Information has significant value and/or is commercially sensitive and unauthorised	Same as Confidential plus: • If being sent by e-mail internally, must be encrypted and password protected. Send the password via a separate channel. • If being sent by Post, double envelope with a tamperproof seal, by hand, Royal Mail Special Deliver or a trusted courier named individual.

5 Appendix B – Guidelines

The classification of information must be judged based on its content. The following table provides some examples for guidance:

Classification	**Definition**
PUBLIC	• Company reports. • Sales / marketing material. • Information that has been created for external distribution. • Information released under Post Office Publication Scheme to meet the requirements of the Freedom of Information Act.
INTERNAL	• General Policies. • General Guidelines. • HR Policy manual. • Organisational charts. • Appointment books / diaries.
CONFIDENTIAL	• Tender documents (ITT and PQQ). • Tactical business plans. • Most financial information (P&L, budgets, invoices, expenses). • Most audit reports. • Design / Technical documentation (LLD, HLD or TIS). • Personal data as defined by The Data Protection Act 2018 (including customer and staff personal data). • Threat and vulnerability assessments and Information Security Health Check (ISHC) results.
STRICTLY CONFIDENTIAL	• Negotiation strategies. • Critical / strategic business plans. • Tender bids. • Most legal information. • Card Holder data as defined by Payment Card Industry-Data Security Standards (PCI-DSS). • Special category personal data as defined by the Data Protection Act 2018.

6 Appendix C – Caveats or Descriptors

It is sometimes necessary to add a caveat to a classification. The table below provides a list of the acceptable caveats which can apply to any level of classification.

Caveat	Descriptions
XXXXX ONLY	For limiting a document set to a specific audience, such as BOARD or GE. E.g. CONFIDENTIAL BOARD ONLY.
UNTIL xx/xx/xx	For limiting the time that a higher classification applies, such as release of company results which become public at a release date but are STRICTLY CONFIDENTIAL before the specified date. E.g. STRICTLY CONFIDENTIAL UNTIL 24/06/2018
WHEN COMPLETE	For forms and other template documents which in themselves do not require a classification, but once the data has been entered into them change to the specified classification. E.g. CONFIDENTIAL WHEN COMPLETE.
LEGAL PRIVILEGE	When the document is written by a professional legal advisor and will continue to protect the contents from being disclosed without permission. E.g. CONFIDENTIAL – LEGAL PRIVILEGE
INVESTIGATION	Used to cover investigations by HR or security to ensure the data contained is not disclosed. E.g. STRICTLY CONFIDENTIAL – INVESTIGATION.

POL00362911

7 Where to go for help

7.1 Additional Policies

This standard is part of the Cyber Security Policy framework. The full set can be found at:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

7.2 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.

7.3 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 Cyber Security Team via GRO

8 Version Control

8.1 Version Control

Date	Version	Updated by	Change Details
04/11/2015	0.1	ISAG	Initial Draft in new format
12/05/2016	0.2	ISAG	Edits after team review
13/05/2016	0.3	ISAG	Minor updates
16/05/2016	1.0	ISAG	Final document and release
10/06/2016	1.1	ISAG	Added caveats description
05/06/2018	1.2	IPA	Changed to new format, minor editorial changes to account for changes in Post Office Structure.
05/07/2018	1.3	ITS	Minor edits
7/04/2020	1.4	Cyber Security	Converted to new document format.
12/06/2020	1.4	Cyber Security	Approved by ISC
28/07/2021	1.5	Cyber Compliance	Final version for approval
02/08/2021	2.0	Cyber Compliance	Approved by ISC
04/04/2023	2.1	Cyber Compliance	Updated the minimum controls to align with the UCF
25/04/2023	2.2	Cyber Complinace	CSF approval for publication

8.2 Standard Approval

Standard Owner:	Chief Information Security Officer
Standard Author:	Ehtsham Ali
Approved by CSF:	25/04/2023
Next review:	25/04/2024