Cyber Security Standard

Asset Management 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 Asset Management Standard is to provide a structured and consistent approach to the management of all Post Office logical and physical assets (including software assets).

1.3 Core Principles

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

- Assets will be managed securely through their lifecycle
- Assets require ownership
- Asset registers will be kept up to date
- Assets will be disposed of securely

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 Office's 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
PHT0660	Control the transiting and internal distribution or external distribution of assets.	Obtain management authorization for restricted storage media transit or distribution from a controlled access area. Transport restricted media using a delivery method that can be tracked.
PHT0663	Restrict physical access to distributed assets.	Protect electronic storage media with physical access controls.
PHT0665	Establish, implement, and maintain a media protection policy.	Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media Disseminate and communicate the media protection policy to interested personnel and affected parties.
PHT0667	Establish, implement, and maintain removable storage media controls.	Control access to restricted storage media. Physically secure all electronic storage media that store restricted data or restricted information. Logically secure any associated data using the appropriate level of encryption in line with the classification of the data. Control the storage of restricted storage media. - CTRL0020583

POL00362907

		Removable media is protected and its use restricted according to policy.
PHT0674	Establish, implement, and maintain off-site physical controls for all distributed assets.	Establish, implement, and maintain asset removal procedures or asset decommissioning procedures. Prohibit assets from being taken off-site absent prior authorisation. Protect distributed assets against theft. Attach asset location technologies to distributed assets. Employ asset location technologies in accordance with applicable laws and regulations.
PHT0679	Establish, implement, and maintain end user computing device security guidelines.	Establish, implement, and maintain a locking screen saver policy.
PHT0681	Establish, implement, and maintain mobile device security guidelines.	Remote lock any distributed assets reported lost or stolen. Remote wipe any distributed asset reported lost or stolen. POL data must not be processed on non POL assets unless the user is accessing POL provided services Removable media must be encrypted when storing POL data in accordance with the classification of the data.

PHT0682	Separate systems that transmit, process, or store restricted data from those that do not by deploying physical access controls.	The organization must keep sensitive information separate from other information to the maximum extent possible
PHT0683	Establish, implement, and maintain asset return procedures.	Require the return of all assets upon notification an individual is terminated.
PHT0685	Establish, implement, and maintain a clean desk policy.	Establish, implement, and maintain a clear screen policy. Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.
PHT0880 CTRL0020614	Establish, implement, and maintain a capacity management plan.	Establish, implement, and maintain a capacity planning baseline. - CTRL0020615 Establish, implement, and maintain future system capacity forecasting methods. Align critical Information Technology resource availability planning with capacity planning. Provide excess capacity or redundancy to limit any effects of a Denial of Service attack. - CTRL0020727 Utilize resource capacity management controls. The organisation must Identify availability and capacity implications of changing business needs and improvement opportunities. Use modelling techniques to validate availability, performance and capacity plans.

PHT0990	Establish, implement, and maintain an Asset Management program.	The organisation must have an asset management policy that details how the asset lifecycle is managed. This includes all the steps from procurement to disposal to ensure assets are fully utilised, accounted for and physically protected Assign an information owner to organizational assets, as necessary.
PHT0992	Establish, implement, and maintain classification schemes for all systems and assets.	Apply security controls to each level of the information classification standard. Define confidentiality controls. Establish, implement, and maintain the systems' availability level. CTRL0020669 Define integrity controls. Establish, implement, and maintain the systems' integrity level. Define availability controls
PHT0999	Classify assets according to the Asset Classification Policy.	Apply asset protection mechanisms for all assets according to their assigned Asset Classification Policy. CTRL0020563 Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality and business value.
PHT1001	Establish, implement, and maintain an asset inventory.	Establish, implement, and maintain an Information Technology inventory with asset discovery audit trails. - CTRL0020647 Include each Information System's system boundaries in the Information Technology inventory. Identify processes, Information Systems, and third parties that transmit, process, or store personal data. Business processes must be in place and documented to manage the life cycle of assets including: Identifying critical Assets Managing assets from procurement to Disposal
PHT1005	Establish, implement, and maintain a hardware asset inventory.	Include network equipment in the Information Technology inventory.
PHT1007	Include interconnected systems and Software as a Service in the Information Technology inventory.	The organisation must maintain and understand how a systems are connected and the cloud resources being used need to be inventoried.

PHT1008	Include software in the Information Technology inventory.	Software platforms and applications within the organization are inventoried.
PHT1009	Establish, implement, and maintain a storage media inventory.	Inventory logs must be properly maintained for all media Media inventories must be conducted at least annually Inventories of backup media, storage location, and access controls for the media or physical location
PHT1010	Establish, implement, and maintain a records inventory and database inventory.	The organization should maintain an accurate inventory of all deployed databases, along with their contents. Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data An inventory of information and other associated assets, including owners, should be developed, and maintained
PHT1011	Record the make, model of device for applicable assets in the asset inventory.	Record the physical location for applicable assets in the asset inventory. Record the manufacturer's serial number for applicable assets in the asset inventory. Record the related business function for applicable assets in the asset inventory. Record the owner for applicable assets in the asset inventory. Record all changes to assets in the asset inventory.
PHT1017	Establish, implement, and maintain a software accountability policy.	Establish, implement, and maintain software asset management procedures. Establish, implement, and maintain software license management procedures. - CTRL0020662
PHT1020	Establish, implement, and maintain a system redeployment program.	Wipe all data on systems prior to when the system is redeployed or the system is disposed. Transfer legal ownership of assets when the system is redeployed to a third party. - CTRL0020747
PHT1023	Establish, implement, and maintain a system disposal program.	It is necessary to formulate a disposal plan for the system, clarify the disposal procedure, and discard it with approval from the person in charge of operation and the user's department The organisation shall define system disposal procedures

		Where data assets are encrypted the encryption keys should be destroyed to prevent access. The data must be deleted by the supplier as per contract, Where data is not encrypted the supplier has to provide evidence that the data has been destroyed in line with best practice (as per contract) When data is no longer required the information must be destroyed in a secure manner and in accordance with the data retention policy and best practice subject to the classification of the data
PHT1024 CTRL0020632	Establish, implement, and maintain a system preventive maintenance program.	Establish and maintain maintenance reports. CTRL0020606 The organisation must document its approach to maintaining assets that support critical services. This needs to includes the steps taken to maximise the reliability and availability of the assets to support business need.
PHT1026	Maintain contact with the device manufacturer or component manufacturer for maintenance requests.	Obtain justification for the continued use of system components when third party support is no longer available.
PHT1028	Control remote maintenance according to the system's asset classification.	Approve all remote maintenance sessions. CTRL0020564 Log the performance of all remote maintenance. CTRL0020705
PHT1031	Conduct maintenance with authorized personnel.	Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access.
PHT1032	Perform periodic maintenance according to organizational standards.	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.
PHT1033	Disassemble and shut down unnecessary systems or unused systems.	It is necessary to make sure that the system has completely ceased operations prior to the start of disposal The organization must develop a hardened Standard Operating Environment for servers and workstations that includes removing unnecessary software, operating system components, and hardware

PHT1034 CTRL0020721	Dispose of hardware and software at their life cycle end.	Assets are formally managed throughout removal, transfers and disposition.
PHT1035	Review each system's operational readiness.	When a system transitions to a production environment, unplanned modifications to the system occur. If changes are significant, a modified test of security controls, such as configurations, are needed to ensure the integrity of the security controls.

4 Where to go for help

4.1 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

4.2 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.

4.3 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 cyber GRO

5 Version Control

5.1 Version Control

Date	**Version**	**Updated by**	**Change Details**
24/07/2019	0.1	IPA & IT Security	First draft for review
04/01/2020	1.0	IT Security	Final draft version for approval
12/06/2020	1.0	Cyber Security	Approved by ISC
28/07/2021	1.1	Cyber Compliance	Final draft version for approval
02/08/2021	2.0	Cyber Compliance	Approved by ISC
23/11/2022	2.1	Cyber Compliance	Update to align with control framework UCF
25/04/2023	2.2	Cyber Compliance	CSF Approval for publication

5.2 Standard Approval

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