POL00362909

Cyber Security Standards

Cyber and Information Security Standard

Version – V2.2

POL00362909

POL00362909

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 Cyber and Information Security Standard is to provide a structured approach to maintaining the Confidentiality, Integrity and Availability of Post Office data.

1.3 Core Principles

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

- Minimise the likelihood that Post Office's information assets will be subject to risks associated with theft, loss, misuse, damage or abuse of these information assets, whether intentional or unintentional, by aiding in preserving their confidentiality, integrity and availability.
- Ensure that employees remain aware of their responsibilities.
- Ensure on-going threat awareness, compliance and continual improvement of information security processes within Post Office.
- Meeting Post Office's contractual, legal and regulatory compliance requirements.

1.4 Application

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

POL00362909

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 policy/standard.

POL00362909

3 Minimum Controls

The table below sets out the relationships between identified risk, and the required minimum control standards.

Control Ref	Control	Attestation Guidance
PHT0002	Analyze organizational objectives, functions, and activities.	Analyze the business environment in which the organization operates. Identify the internal factors that may affect organizational objectives. Include existing information in the analysis of the internal business environment. Include resources in the analysis of the internal business environment. Include strengths and weaknesses in the analysis of the internal business environment. Align assets with business functions and the business environment. Disseminate and communicate the organization's business environment and place in its industry sector. Monitor for changes which affect organizational objectives in the internal business environment.
PHT0011	Analyze the external environment in which the organization operates.	Monitor for changes which affect organizational strategies in the external environment. Monitor for changes which affect organizational objectives in the external environment. Include opportunities in the analysis of the external environment. Include technology in the analysis of the external environment. Cyber and Information Security must be embedded into change and project management processes.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0016	Conduct a context analysis to define objectives and strategies.	The purpose of the business analysis practice is to analyse a business or some element of it, define its associated needs, and recommend solutions to address these needs and/or solve a business problem, which must facilitate value creation for stakeholders.
PHT0017	Establish, implement, and maintain organizational objectives.	Evaluate organizational objectives to determine impact on other organizational objectives. Identify events that may affect organizational objectives. Identify conditions that may affect organizational objectives. Identify requirements that could affect achieving organizational objectives. Identify opportunities that could affect achieving organizational objectives.
PHT0023	Prioritize organizational objectives.	Disseminate and communicate organizational objectives to all interested personnel and affected parties.
PHT0025	Document and communicate the linkage between organizational objectives, functions, activities, and general controls.	Identify threats that could affect achieving organizational objectives. CTRL0020676 Identify how opportunities, threats, and external requirements are trending. Review the organization's approach to managing information security, as necessary.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0029	Identify all interested personnel and affected parties.	Analyze and prioritize the requirements of interested personnel and affected parties. A list of appropriate contacts from the relevant authorities for Cyber and Information Security must be created and maintained. A list of membership to any special interest groups must be created and maintained.
PHT0031	Establish, implement, and maintain an information classification standard.	Classify the sensitivity to unauthorized disclosure or modification of information in the information classification standard. Classify the criticality to unauthorized disclosure or modification of information in the information classification standard. Classify the value of information in the information classification standard. Classify the legal requirements of information in the information classification standard.
PHT0036	Establish, implement, and maintain a data classification scheme.	An appropriate classification scheme will need to be enforced, such as the Information Classification Standard.
PHT0037	Establish, implement, and maintain an Information and Infrastructure Architecture model.	The purpose of the architecture management practice is to provide an understanding of all the different elements that make up an organization and how those elements interrelate, enabling the organization to effectively achieve its current and future objectives. Establish, implement, and maintain sustainable infrastructure planning.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0039	Monitor regulatory trends to maintain compliance.	Subscribe to a threat intelligence service to receive notification of emerging threats. Disseminate and communicate emerging threats to all interested personnel and affected parties. Disseminate and communicate updated guidance documentation to interested personnel and affected parties upon discovery of a new threat. All relevant legislative statutory, regulatory, contractual requirements and the approach to meet these requirements shall be explicitly identified, documented, and kept up to date for all POL Systems.
PHT0043	Establish, implement, and maintain a Quality Management framework.	Correct errors and deficiencies in a timely manner. Document the deficiencies in a deficiency report that were found during Quality Control and corrected during Quality Improvement. Include program documentation standards in the Quality Management program. Include system testing standards in the Quality Management program.
PHT0054	Establish and maintain the scope of the organizational compliance framework and Information Assurance controls.	Identify roles, tasks, information, systems, and assets that fall under the organization's mandated Authority Documents. Establish, implement, and maintain a policy and procedure management program. Include requirements in the organization's policies, standards, and procedures. Analyze organizational policies, as necessary. Establish and maintain a list of compliance documents. Document organizational procedures that harmonize external requirements, including all legal requirements. Establish, implement, and maintain full documentation of all policies, standards, and procedures that support the organization's compliance framework.

POL00362909

Control Ref	Control	Attestation Guidance
		Disseminate and communicate the organization's policies, standards, and procedures to all interested personnel and affected parties. ISMS must be aligned to ISO27001/02 and independently assessed on an annual basis.
PHT0063	Publish, disseminate, and communicate a Statement on Internal Control, as necessary.	Include management's assertions on the effectiveness of internal control in the Statement on Internal Control. Include confirmation of any significant weaknesses in the Statement on Internal Control. Include roles and responsibilities in the Statement on Internal Control Include limitations of internal control systems in the Statement on Internal Control.
PHT0068	Approve all compliance documents.	Align the list of compliance documents with external requirements. Assign the appropriate roles to all applicable compliance documents. Establish, implement, and maintain a compliance exception standard. Include all compliance exceptions in the compliance exception standard. Review the compliance exceptions in the exceptions document, as necessary.
PHT0074	Disseminate and communicate compliance documents to all interested personnel and affected parties.	Disseminate and communicate any compliance document changes when the documents are updated to interested personnel and affected parties.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0076	Define the Information Assurance strategic roles and responsibilities.	Establish and maintain a compliance oversight committee. Provide critical project reports to the compliance oversight committee in a timely manner. Assign the corporate governance of Information Technology to the compliance oversight committee. Involve the Board of Directors or senior management in Information Governance. Address Information Security during the business planning processes. Assign reviewing and approving Quality Management standards to the appropriate oversight committee. Governance and Risk Management processes must be in place and an assessment must be completed for all systems annually and during major change. Conflicting roles must be documented defining any that require segregation from other roles.
PHT0083	Define and assign the Chief of Risk's Information Assurance roles and responsibilities.	Top management and oversight bodies, where applicable, should ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to risk management are assigned and communicated at all levels of the organization
PHT0084	Establish, implement, and maintain a strategic plan.	Establish, implement, and maintain a decision management strategy. Include criteria for risk tolerance in the decision making criteria. Include criteria for selecting objectives and strategies in the decision making criteria. Include criteria for setting priorities in the decision making criteria. Align organizational objectives with compliance objectives in the decision-making criteria.

POL00362909

Control Ref	Control	Attestation Guidance
		Align organizational objectives with performance targets in the decision-making criteria. Align organizational objectives with the acceptable residual risk in the decision-making criteria. Identify and document the events that initiate the decision management strategy. Create additional decision-making criteria to achieve organizational objectives, as necessary. Document and evaluate the decision outcomes from the decision-making process. Cyber and Information security requirements for mitigating the risks within the supplier must be assessed prior to the supplier entering into a contract with Post Office or having access to Post Office Data. A supplier management process must in place.
PHT0095	Establish, implement, and maintain a Strategic Information Technology Plan.	Include business continuity objectives in the Strategic Information Technology Plan. Align business continuity objectives with the business continuity policy. Business Continuity Planning and Disaster Recovery must be in place and tested annually for the continuity of Information Security Management during a crisis or disaster. Backup copies of information, software and system images shall be taken as per an agreed schedule and tested regularly. Business impact assessment must performed on an annual basis to gain an understanding of the impact of any adverse event.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0098	Use a risk-based approach to adapt the Strategic Information Technology Plan to the business's needs.	Mirror the organization's business strategy during Information Technology planning in the Strategic Information Technology Plan.
PHT0100	Establish, implement, and maintain tactical Information Technology plans in support of the Strategic Information Technology Plan.	Establish, implement, and maintain tactical Information Technology plans derived from the Strategic Information Technology Plan. Document how each Information Technology project plan directly or indirectly supports the Strategic Information Technology Plan. Document the business case and return on investment in each Information Technology project plan. Document all desired outcomes for a proposed project in the Information Technology project plan. Assign senior management to approve business cases. Include milestones for each project phase in the Information Technology project plan. All systems holding or processing Post Office information shall operate anti-malware protection regardless of the underling operating system. The systems used shall be the current best practice offerings. Anti-virus program must capable of detecting, removing, and protecting against all known types of malicious software and Post Office must be maintained as follows: • keep current, • Perform periodic scans • Generate audit logs which are retained according to the data retention policy.

POL00362909

Control Ref	Control	Attestation Guidance
		• Anti-virus mechanisms are actively running and cannot be disabled or altered by users.
PHT0107	Document lessons learned at the conclusion of each Information Technology project.	Disseminate and communicate the Information Technology Plans to all interested personnel and affected parties. Monitor and evaluate the implementation and effectiveness of Information Technology Plans. Establish and maintain an Information Technology plan status report that covers both Strategic Information Technology Plans and tactical Information Technology plans Include the Information Governance Plan in the Strategic Information Technology Plan. Review and approve the Strategic Information Technology Plan at the level of senior management or the Board of Directors.
PHT0113	Establish, implement, and maintain a Governance, Risk, and Compliance awareness and training program.	Establish and maintain a rapport with business and technical communities throughout the organization to promote the value and importance of Information Security. All Staff must undergo annual Cyber and Information Security training.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0115	Establish, implement, and maintain a financial management program.	Establish, implement, and maintain financial reports.
PHT0117	Establish, implement, and maintain communication protocols.	Align the information being disseminated and communicated with the communication requirements according to the organization's communication protocol. Assess the effectiveness of the communication methods used in the communication protocol. Include input from interested personnel and affected parties as a part of the organization’s communication protocol. Report to management and stakeholders on the findings and information gathered from all types of inquiries. Establish and maintain the organization's survey method. Establish, implement, and maintain warning procedures that follow the organization's communication protocol. Establish, implement, and maintain alert procedures that follow the organization's communication protocol.
PHT0125	Establish, implement, and maintain an external reporting program.	Monitor service availability when implementing the service management monitoring and metrics program. Compare the performance metrics of service availability against their targets, as necessary.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0399	Establish, implement, and maintain a compliance monitoring policy.	Establish, implement, and maintain an approach for compliance monitoring. Establish, implement, and maintain risk management metrics. Identify information being used to support the performance of the governance, risk, and compliance capability. Monitor personnel and third parties for compliance to the organizational compliance framework. Identify and document instances of non-compliance with the compliance framework. Determine the causes of compliance violations. Determine if multiple compliance violations of the same type could occur. Review the effectiveness of disciplinary actions carried out for compliance violations. Carry out disciplinary actions when a compliance violation is detected. Align disciplinary actions with the level of compliance violation. Establish, implement, and maintain a security program metrics program. Report on the policies and controls that have been implemented by management. Establish, implement, and maintain a Business Continuity metrics program. Establish, implement, and maintain an Information Security metrics program.
PHT0414	Establish, implement, and maintain a metrics policy.	Establish, implement, and maintain a metrics standard and template. Monitor compliance with the Quality Control system. Establish, implement, and maintain a policies and controls metrics program. Monitor the supply chain for Information Assurance effectiveness.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0419	Establish, implement, and maintain a technical measurement metrics policy.	Establish, implement, and maintain a network management and firewall management metrics program. Establish, implement, and maintain a network activity baseline. Establish, implement, and maintain an incident management and vulnerability management metrics program. Report on the percentage of vulnerability assessment findings that have been addressed since the last reporting period. Cyber and Information security events must be assessed and it shall be decided if they are to be classified as information security incidents. Cyber and Information security incidents must be responded to in accordance with the documented procedures.
PHT0424	Establish, implement, and maintain a log management program.	Restrict access to logs to a need to know basis. Restrict access to audit trails to a need to know basis. Back up audit trails according to backup procedures. Copy logs from all predefined hosts onto a log management infrastructure. Protect logs from unauthorized activity. Archive the audit trail in accordance with compliance requirements.
PHT0431	Monitor the performance of the governance, risk, and compliance capability.	Monitor and periodically evaluate the performance of the capability to ensure it is designed and operated to be effective, efficient, and responsive to change.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0432	Establish, implement, and maintain a corrective action plan.	Include monitoring in the corrective action plan.
PHT0434	Report compliance monitoring statistics to the Board of Directors and other critical stakeholders, as necessary.	Report actions taken on known security issues to the Board of Directors or Senior Executive Committee on a regular basis.
PHT0613	Establish, implement, and maintain an application security policy.	Establish, implement, and maintain a virtual environment and shared resources security program.
PHT0849	Establish, implement, and maintain a security awareness program.	Establish, implement, and maintain a security awareness and training policy. Establish, implement, and maintain security awareness and training procedures. Disseminate and communicate the security awareness and training procedures to interested personnel and affected parties.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0853	Document security awareness requirements.	Include updates on emerging issues in the security awareness program. Include cybersecurity in the security awareness program. Include training based on the participants' level of responsibility and access level in the security awareness program. Include a requirement to train all new hires and interested personnel in the security awareness program. Disseminate and communicate the security awareness program to all interested personnel and affected parties. Train all personnel and third parties on how to recognize and report security incidents. Require personnel to acknowledge, through writing their signature, that they have read and understand the organization's security policies.
PHT0861	Conduct secure coding and development training for developers.	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory
PHT0862	Conduct tampering prevention training.	Include the mandate to refrain from installing, refrain from replacing, and refrain from returning any asset absent verification in the tampering prevention training. Include how to identify and authenticate third parties claiming to be maintenance personnel in the tampering prevention training. Include how to report tampering and unauthorized substitution in the tampering prevention training. Include how to prevent physical tampering in the tampering prevention training.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0898	Document the organization's business processes.	The organization need to create an initial high-level overview of its activities and business relationships, the sustainability context in which these occur, and an overview of its stakeholders.
PHT0899	Establish, implement, and maintain a Governance, Risk, and Compliance framework.	Disseminate and communicate updates to the Governance, Risk, and Compliance framework to interested personnel and affected parties. Acquire resources necessary to support Governance, Risk, and Compliance. Implement the prioritized plan for updating the Governance, Risk, and Compliance framework. Evaluate the use of technology in supporting Governance, Risk, and Compliance capabilities. Analyze the effect of the Governance, Risk, and Compliance capability to achieve organizational objectives. Assign accountability for maintaining the Governance, Risk, and Compliance framework. Assign defining the program for disseminating and communicating the Governance, Risk, and Compliance framework.
PHT0907	Establish, implement, and maintain a positive information control environment.	Define the elements of a control environment for IT, aligned with the enterprise's management philosophy and operating style

POL00362909

Control Ref	Control	Attestation Guidance
PHT0908	Establish, implement, and maintain an internal control framework.	Measure policy compliance when reviewing the internal control framework. Assign ownership of the internal control framework to the appropriate organizational role. Assign resources to implement the internal control framework. Define and assign the roles and responsibilities for interested personnel and affected parties when establishing, implementing, and maintaining the internal control framework. Include procedures for continuous quality improvement in the internal control framework.
PHT0923	Establish, implement, and maintain an information security program.	Include technical safeguards in the information security program. Include access control in the information security program. Review and approve access controls, as necessary. Include operations management in the information security program. Include physical security in the information security program. Include a continuous monitoring program in the information security program. Include how the information security department is organized in the information security program. Include risk management in the information security program. Include mitigating supply chain risks in the information security program. Monitor and review the effectiveness of the information security program. Establish, implement, and maintain an information security policy. Align the information security policy with the organization's risk acceptance level. Include a commitment to the information security requirements in the information security policy. Include information security objectives in the information security policy. Approve the information security policy at the organization's management level or higher. Document the roles and responsibilities for all activities that protect restricted data in the information security procedures.

POL00362909

Control Ref	Control	Attestation Guidance
PHT0965	Establish, implement, and maintain nondisclosure agreements.	Require interested personnel and affected parties to sign nondisclosure agreements. Establish, implement, and maintain a use of information agreement. Confidentiality or non-disclosure agreements must be in place when sharing Post Office data with a third party.
PHT0968	Implement and comply with the Governance, Risk, and Compliance framework.	Establish, implement, and maintain consequences for non-compliance with the organizational compliance framework. Comply with all implemented policies in the organization's compliance framework. Provide assurance to interested personnel and affected parties that the Governance, Risk, and Compliance capability is reliable, effective, efficient, and responsive. Review systems for compliance with organizational information security policies. Disseminate and communicate the Governance, Risk, and Compliance framework to all interested personnel and affected parties.

POL00362909

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

POL00362909

5 Version Control & Approval

5.1 Version Control

Date	Version	Updated by	Change Details
24/07/2019	0.1	IPA & IT Security	First redraft for review – replaces the Cyber and Information Security policy
22/01/2020	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
10/04/2023	2.1	Cyber Compliance	Updated the controls to align with UCF.
25/04/2023	2.2	Cyber Compliance	CSF approval for publication

5.2 Standard Approval

Standard Owner: Chief Information Security Officer

Standard Author: Ehtsham Ali

Approved by CSF: 25/04/2023

Next review: 25/04/2024