POL00362918

Cyber Security Standard

Vulnerability Standard

Version – V1.4

POL00362918

POL00362918

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 this standard is to define how Post office will manage the potential Vulnerabilities within its information systems to ensure that these potential vulnerabilities are discovered and remediated before they can be exploited.

1.3 Core Principles

The objective of this standard is to achieve the following:

- Define how Post Office will identify and remediate vulnerabilities within its information systems
- Ensure that the proportionate and appropriate management of information security risks are performed to mitigate the threat of vulnerabilities being exploited.

1.4 Application

This standard applies to all people, systems, networks and services used to support the Post office including those managed and maintained by the post office as well as those managed, maintained and supported by a third party supplier on behalf of Post Office. It includes both technical and non-technical vulnerabilities, involving systems, applications, networks, location, people and process.

POL00362918

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.

POL00362918

3 Minimum Controls

The table below sets out the minimum control standards.

Control Ref	Control Objective	Control Guidelines
PHT0351	Establish, implement, and maintain a testing program	The Post Office maintains an enterprise vulnerability program owned by the Cyber Security Team. The program manages Vulnerabilities by: • Performing internal and external Vulnerability Assessments (By using tools such as Nessus, Tennable and Qualys) • Performing scoped penetration tests in line with contractual, compliance and regulatory requirements • Perform remediation based on the criticality and potential risk to POL, it's suppliers and partners impacted by the vulnerability identified
PHT0352	Conduct Red Team exercises, as necessary.	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively The organisation conducts, either by itself or by an independent third-party, periodic penetration testing and red team testing on the organization's network, internet-facing applications or systems, and critical applications to identify gaps in cybersecurity defences
PHT0353	Test security systems and associated security procedures, as necessary	Employ third parties to carry out testing programs, as necessary. Regularly test security systems and processes Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems
PHT0355	Define the test requirements for each testing program.	Security testing (including reviews) to identify vulnerabilities and confirm information security requirements have been met. The nature of testing would be commensurate with the scope of the change and the sensitivity and criticality of the impacted information asse
CTRL002073 PHT0356	Scan organizational networks for rogue devices.	Scan the network for wireless access points. Implement incident response procedures when rogue devices are discovered.
PHT0359	Define the test frequency for	The testing frequency must be agreed and documented based on a risk based

POL00362918

Control Ref	Control Objective	Control Guidelines
	each testing program.	approach
PHT0360	Disseminate and communicate the testing program to all interested personnel and affected parties.	The Independent penetration test reports must be supplied to Cyber Security for review
PHT0361	Establish, implement, and maintain a penetration test program.	A penetration testing methodology must be implemented that is based on industry-accepted penetration testing practices
PHT0362	Align the penetration test program with industry standards.	After the Independent Assessment /Penetration test has been completed: • The Independent penetration test reports must be supplied to Cyber Security for review, • A remediation plan must be created where findings are identified, • The remediation plan must be agreed with Cyber Security. All vulnerabilities have to be presented with a CVSS V3 score. When there is no permanent solution, or the fix timescale has lapsed, both the Cyber Security and Risk Management teams have to be informed and a risk management process has to be implemented as per Post Office Risk Policy."
PHT0364	Establish, implement, and maintain a penetration testing methodology that validates scope-reduction controls through network segmentation.	Implement a methodology for penetration testing that includes the following: - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) - Includes coverage for the entire CDE perimeter and critical systems - Includes testing from both inside and outside the network
PHT0365	Retain penetration test results according to internal policy.	All information gathered during the course of testing must be treated as confidential and therefore handled and transmitted as such.
PHT0366	Retain penetration test remediation action records	All information gathered during the course of testing must be treated as confidential and therefore handled and transmitted as such.

POL00362918

Control Ref	Control Objective	Control Guidelines
	according to internal policy.	
PHT0367	Perform penetration tests, as necessary.	Independent penetration testing of systems must be conducted based on their regulatory status (e.g. PCI-DSS), criticality or risk profile. Key systems, and those covered by PCI DSS, must be tested annually, along with all Internet facing systems. All other systems should be tested based upon their risk profile. All systems must be tested on the occasion of either a significant change or an incident that changes the threat landscape of the environment. Perform internal penetration tests, as necessary. Perform external penetration tests, as necessary.
PHT0370	Include coverage of all in scope systems during penetration testing.	Perform network-layer penetration testing on all systems, as necessary. Perform application-layer penetration testing on all systems, as necessary. Perform penetration testing on segmentation controls, as necessary.
PHT0374	Correct vulnerabilities and repeat penetration testing.	Examine the penetration testing results to verify the exploitable vulnerabilities that were detected were corrected and the penetration tests were repeated to confirm the vulnerability was corrected Exploitable vulnerabilities that are detected during the penetration testing must be corrected and the penetration test must be repeated to verify the vulnerabilities are corrected
PHT0375	Establish, implement, and maintain a vulnerability assessment program.	Conduct vulnerability assessments or penetration tests for systems at least annually A comprehensive vulnerability management process must exist that includes identifying and mitigating software vulnerabilities and hardware vulnerabilitie s
PHT0376	Perform vulnerability scans, as necessary.	Repeat vulnerability scanning, as necessary. Identify and document security vulnerabilities. Rank discovered vulnerabilities.
PHT0380	Assign vulnerability scanning to qualified personnel or external third parties.	"An independent external vulnerability assessment must be considered as part of every IT Project and if a scan is deemed as required it must, as a minimum, be performed before an information system can 'Go-Live' and become operational.

POL00362918

Control Ref	Control Objective	Control Guidelines
		Independent external vulnerability assessments must be performed at least quarterly for every externally facing system that store, process or transmit cardholder data and yearly for all other externally facing systems. An independent external vulnerability assessment must be performed when there is a major change to an externally facing system, if there is a change to the operating environment or when a new information risk is identified. The independent external vulnerability assessments can only be conducted by an approved, trusted and qualified third party. A third party can perform their own assessments to reduce the cost of tracking remediation, however these can't be relied on, an independent test has to be performed to ensure all vulnerabilities have been identified."
PHT0381	Maintain vulnerability scan reports as organizational records.	The security function should have updated status regarding numbers of unmitigated, critical vulnerabilities, for each department/division, plan for mitigation and should share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually
PHT0382	Correlate vulnerability scan reports from the various systems.	The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors
PHT0383	Perform internal vulnerability scans.	Internal vulnerability assessments must be run across Post Office Systems at least monthly. As a minimum this must be performed for all internet facing systems and assets. Where systems contain strictly confidential information it may be necessary to run the scans more frequently. Scan results shall be shared with Cyber Security via integration into Post Office Service Now or until integration built via a secure method to information.security GRO and vulnerabilities need to be assessed,

POL00362918

Control Ref	Control Objective	Control Guidelines
		prioritised and remediated according to business impact and criticality.
PHT0384	Repeat vulnerability scanning after an approved change occurs.	Within 30 days of the change
PHT0385	Perform external vulnerability scans on the organization's systems.	External vulnerability scans must be performed at least monthly. Employ an approved third party to perform external vulnerability scans on the organization's systems.
PHT0387	Perform vulnerability assessments, as necessary.	Conducting a vulnerability assessment for each vulnerability and calculating the probability that it will be exploited. Evaluating policies, procedures, standards, training, physical security, quality control and technical security in this regard Conduct regular ICT security audits, scans and tests to detect vulnerabilities and non-compliance with organisational standards
PHT0388	Review applications for security vulnerabilities after the application is updated.	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: - Reviewing public-facing web applications via manual or automated application vulnerability security At least once every 12 months and after significant changes
PHT0389	Perform penetration tests and vulnerability scans in concert, as necessary.	include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems Recommend mitigation techniques based on vulnerability scan reports. When no fix is available a workaround must be agreed with Cyber Security until a permanent fix is available and implemented. Correct or mitigate vulnerabilities.
CTRL0020624	Establish, implement, and maintain a malicious code	Install security and protection software, as necessary. Scan for malicious code, as necessary.

POL00362918

Control Ref	Control Objective	Control Guidelines
	protection program.	
CTRL0020702	Log and react to all malicious code activity.	It is necessary to take measures in preparation for cases where computer virus infection or malicious program is detected on a computer All anti-virus mechanisms must generate audit logs
PHT0612	Lock antivirus configurations.	Include vulnerability management and risk assessment in the internal control framework. Automate vulnerability management, as necessary.
PHT0916	Include continuous security warning monitoring procedures in the internal control framework.	Include incident alert thresholds in the continuous security warning monitoring procedures.
PHT0918	Include security information sharing procedures in the internal control framework.	Share relevant security information with Special Interest Groups, as necessary.
PHT0920	Include security incident response procedures in the internal control framework.	The organisation should have defined procedures for the escalation of a security incident Verify the responsibility for establishing, documenting, and distributing Security Incident Response and escalation procedures has been formally assigned in the Information Security policies and procedures The Information Security policies and procedures must formally assign an individual or team the responsibilities for establishing, documenting, and distributing Security Incident Response and escalation procedures to ensure all situations are handled timely and effectively
PHT0921	Authorize and document all exceptions to the internal control framework.	The appropriateness of approved exceptions and the assessment of the risks resulting from this are reviewed by an independent third party at least once a year as to whether they reflect a realistic picture of the current and future expected threat environment regarding information security The entity's system availability and related security policies include providing for handling of exceptions and situations that are not specifically addressed in the system availability and related security policies Instances where the responsible entity cannot conform to its cyber security

POL00362918

Control Ref	Control Objective	Control Guidelines
		policy must be documented as exceptions and authorized by the senior manager or delegate(s)
PHT0922	Disseminate and communicate the internal control framework to all interested personnel and affected parties.	Security policies and operational procedures must be documented, implemented, and communicated to all affected parties

POL00362918

4 Where to go for help

4.1 Additional Policies and Standards

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 IT Helpdesk

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 GRO

POL00362918

5 Version Control & Approval

5.1 Version Control

Date	Version	Updated by	Change Details
25/04/2018	0.1	IT Security	First draft
02/05/2018	0.2	IT Security	Updates
23/05/2018	0.3	IT Security	Updated post peer review
24/05.2018	0.4	IT Security	Updated post further comments
27/05/2018	1.0	IT Security	Final Version Approved
10/11/2021	1.1	Cyber Security	Updated the section 3.2 and 3.3. after discussions with Mark J Cunningham and Dave King
21/07/2022	1.2	Cyber Security	First review and comments
11/11/2022	1.3	Cyber Security	Further review to include new minimum controls
25/04/2023	1.4	Cyber Security	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