POL00362915

Cyber Security Standard

Penetration Testing and Vulnerability Scanning Standard

Version – V1.3

POL00362915

1 Overview 4
1.1 Introduction by the Standard Owner 4
1.2 Purpose 4
1.3 Application 4
1.4 Application 4
2 Policy Framework 6
2.1 Policy Framework 6
2.2 Who must comply? 6
3 Managing Penetration Testing and Vulnerability Scanning 7
3.1 Prepare and Schedule 7
3.2 Perform 7
3.3 Review 7
3.4 Remediate 7
4 Penetration Testing and Vulnerability Scanning 9
4.1 Penetration Testing 9
4.2 Vulnerability Testing 9
4.3 Penetration Test and Scanning Criteria 10
4.4 Additional Requirements 10
4.5 Payment Card Industry Data Security Standards (PCI DSS) 11
4.6 Remediation 11
4.7 Re-tests and Scans 11
4.8 Penetration Test Document Set 12
4.9 Penetration Test Suppliers – Minimum Requirements 12
5 Where to go for help 13
5.1 Additional Policies and Standards 13
5.2 How to raise a concern 13
5.3 Who to contact for more information 13
6 Version Control & Approval 14
6.1 Version Control 14
6.2 Standard Approval 14

POL00362915

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 Penetration Testing and Vulnerability Scanning Standard is to define a structured and consistent approach when performing penetration and vulnerability tests throughout the Post Office.

Cyber Security, together with the appropriate third-party, penetration tester, System Owner and project management representatives (if applicable), will discuss and agree a remediation plan for all critical, high and medium risk vulnerabilities discovered during testing. In line with the Vulnerability Management Standard, the responsibility for ensuring any identified vulnerabilities are remediated lies with the Business/Product Owner and/or System Owner.

1.3 Core Principles

The objective of this standard is to achieve the following:

- Ensure the confidentiality, integrity and availability of Post Office data.
- Sets out the requirements for effective penetration testing and vulnerability scanning.
- Manage assessment of vendor vulnerability notifications and patches.
- Intelligently manage discovered vulnerabilities.
- Avoid network and/or platform downtime.
- Meet Post Offices' contractual, legal and regulatory requirements.
- Preserve corporate image and customer loyalty.
- Protect operational platforms throughout Post Office.
- Incorporate additional regulatory requirements, when appropriate.
- Effective management and remediation of all material identified risks.

1.4 Application

This policy applies to Post Office permanent employees, temporary employees, agency contractors, consultants and anyone else working on behalf of the Post Office accessing Post Office data and aligns to the requirements of the Cyber and Information Security Policy.

Post Office information assets and environments include, but are not limited to:

POL00362915

- Critical business environments.
- Business applications (including those under development).
- Information assets and systems.
- Network devices and communications.
- Any Post Office web presence (including white labelled sites).

POL00362915

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.

POL00362915

3 Managing Penetration Testing and Vulnerability Scanning

3.1 Prepare and Schedule

Cyber Security will collate high level architectural designs, data flow diagrams and questionnaires received from relevant third party suppliers and send to relevant party undertaking the test or scan.

For penetration test and initial scans, scoping meeting(s) will be arranged with relevant parties, including third party suppliers.

Cyber Security must review and agree any proposal with third party suppliers following scoping meeting.

Third party suppliers must agree and sign off test dates and dependencies. Deviation to arranged dates can lead to cancellation costs to Post Office.

Cyber Security schedules penetration tests for systems belonging to the Top 20 Suppliers annually, regular vulnerability scans and penetration tests on new suppliers and systems before go-live. System Owners are responsible for making sure their systems are tested as per the Vulnerability Management Standard.

As part of Payment Card Industry Data Security Standard (PCI DSS) all Post Office systems handling or processing payment cards must be penetration tested annually and scanned quarterly.

3.2 Perform

The agreed partner must perform tests or scans and be operating under an agreed scope.

Cyber Security must receive notification of all vulnerabilities found during testing in the form of a report. Vulnerabilities will be scored using the Common Vulnerability Scoring System (CVSS) – see later section for details.

3.3 Review

Cyber Security will review the report and, if necessary, share the report with relevant third party suppliers who manage the systems that have been penetration tested.

Cyber Security review all vulnerabilities with a CVSS score over 4.0 within the report and discuss with the third party supplier. For details of CVSS scoring see section below.

Third party supplier produces an action plan to remediate the identified vulnerabilities highlighted within the report.

3.4 Remediate

Once the actions detailed in the plan have been completed a re-test or scan of the system must be undertaken to assure the effectiveness of the remediation.

POL00362915

Any outstanding critical/high/medium vulnerabilities not remediated are required to be reported to the Cyber Security Team, business/product owner and Project Manager (if part of a project being delivered).

CVSS	Risk	JIRA Priority	Pen Risk Score	Risk Impact	Risk Likelihood	POL Threat Score (Risk impact X Risk Likelihood)	POL Threat Rating	Fix timescales if discovered within project	Fix timescales if discovered in Live environment	
0.1	Low	Lowest	1.0	1	1	1	very Low	Within 60 Days of go-live	60 Days	
0.2-3.9	Low	Low	2.0 -5.0	1	2 to 5	2 -- 5	Low	Within 60 Days of go-live	60 Days	
				2 to 5	1					
				2	2					
4.0 - 6.9	Medium	Medium	6.0 - 15.0	2	3 to 5	6 -- 10	Medium	Fix within 30 days of go-live (i.e By next release) or will block go-live.	30 Days	Approved Exception Request required if resolution is outside of timescales and product wished to go-live
				3 to 5	2					
				3	3					
7.0 - 8.9	High	High	16.0 - 20.0	3	4 to 5	11 -- 16	High	Now - will block go-live until resolved	7 Days	Approved Exception Request required if resolution is outside of timescales and product wished to go-live
				4 to 5	3					
				4	4					
9.0 - 10.0	Critical	Highest	21.0 - 25.0	4	5	17 - 25	Very High	Now - will block go-live until resolved	Immediately	Approved Exception Request required if resolution is outside of timescales and product wished to go-live
				5	4					
				5	5					

POL00362915

4 Penetration Testing and Vulnerability Scanning

The main objective of penetration testing and scanning is to determine security vulnerabilities within a system. A test or scan also tests Post Office's third party suppliers' information security compliance to ensure they are aligned to the policies and standards produced and authorised by Post Office and best business practices as defined by industry standards in regard to Cyber and Information Security systems.

4.1 Penetration Testing

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.

Detailed documentation of any components requested within the scope of the penetration test must be made available to both the independent third-party tester and Cyber Security. Failure to submit all necessary documentation when requested may impact the accuracy of the scope and delay the submission of a proposal from the penetration test company, which could then delay when the test is conducted. This may have a significant effect on receiving sign-off from Cyber Security during the gating process.

This information will ensure the penetration test company understands how functionality should work and whether results received are expected for the given scenario.

As part of the scoping process the responsible supplier (supplying the service) must provide the penetration testers and Cyber Security with the appropriate documentation, which may include:

- A network diagram depicting all network segments and endpoints in scope for the test.
- Data flow diagram(s) showing data classification levels.

4.2 Vulnerability Testing

Vulnerability testing may be undertaken as part of a penetration test, or through the use of automated or manual tools. Typically these tests will take place at agreed, scheduled, regular intervals to comply with regulatory requirements or risk profile. Following initial scanning and 'filtering' of the results for accuracy, subsequent scans may be limited to reporting only those new or remaining validated vulnerabilities, except where full reporting is a regulatory requirement. For frequency requirements please see the Vulnerability Management Standard

Externally facing systems must be scanned through an Internet hosted service which provides the appropriate certification to meet regulatory requirements.

Internal scans must be conducted as 'authenticated' wherever possible.

All scans must result in the production of a list of all discovered vulnerabilities and must be validated by the supplier being tested. Any dispute over the accuracy of the findings

POL00362915

must be referred to the third party conducting the scan or the vendor of the toolset employed.

4.3 Penetration Test and Scanning Criteria

Activity Description	Guidance Criteria (Not an exhaustive list)
Mandatory penetration test and vulnerability scan to be completed	• External Interfaces. • Web Portals. • Wireless Network Analysis. • Critical Business Processes. • New Business Processes. • Confidential or Strictly Confidential Data. • Amending / New Third Parties or Supplier Connections. • Regulatory Compliance In-Scope. • New Outsourcing Agreement. • Handling or processing payment card information.
Penetration test can be carried out at the next pre-scheduled date	• Internal changes only – no external connectivity involved. • Internal Data. • Non-critical business process. • No Regulatory Compliance aspects.
No penetration test required	• Minor change not involving interfaces or data movement. • Internal interfaces. • Non-critical business process.

4.4 Additional Requirements

The following provides a non-exhaustive list of minimum requirements to be performed and documented when preparing, scheduling and performing a penetration test or vulnerability scan:

- A Business Impact Assessment.
- A Security and Threat Risk Assessment.
- A Privacy Impact Assessment.
- Questionnaire/s issued to the supplier and/or Project Manager as part of the information gathering process, which must be completed before the scoping meeting with the penetration test provider takes place.
- A member of Cyber Security is to be engaged during all stages.
- A qualified QSA is to be engaged where PCI DSS data/information is present within the scope of the environment being tested.
- A qualified technical individual/s with full working knowledge of the environment to be tested (e.g. third party business supplier) must be involved to support the systems during the testing process.
- A representative of Post Office's SISD supplier if requested by Post Office.

POL00362915

4.5 Payment Card Industry Data Security Standards (PCI DSS)

PCI SCC provides general guidance and guidelines for penetration testing. The guidance focuses on the following:

- **Penetration Testing Components:** Understanding of the different components that make up a penetration test and how this differs from a vulnerability scan including scope, application and network-layer testing, segmentation checks, and social engineering.
- **Qualifications of a Penetration Tester**: Determining the qualifications of a penetration tester, whether internal or external, through their past experience and certifications.
- **Penetration Testing Methodologies:** Detailed information related to the three primary parts of a penetration test: pre-engagement, engagement, and post-engagement.
- **Penetration Testing Reporting Guidelines:** Guidance for developing a comprehensive penetration test report that includes the necessary information to document the test as well as a checklist that can be used by the organization or the assessor to verify whether the necessary content is included.

https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf?agreement=true&time=1636046198816

4.6 Cyber Security Remediation

Following a penetration test or vulnerability scan, the supplier engaged to carry out such tests is required to produce a detailed report highlighting and describing all vulnerabilities discovered. An interim report is required within 24 hours of the test completing (in Excel format) and a final full report is required within 5 working days (unless otherwise agreed with Cyber Security) in PDF format.

The System Owner is responsible for making sure that all critical, high and medium findings are remediated within an agreed timescale and before go live of a new system

4.7 Re-tests and Scans

Re-tests or scans are required to provide assurance that vulnerabilities discovered during any penetration tests, ASV and/or VS's have been completely remediated. The schedule for re-tests and scans must be agreed with Cyber Security to ensure they are completed in a timely fashion.

Project Managers will engage with Cyber Security, third party suppliers and penetration test service providers to schedule re-tests or scans.

4.8 Penetration Test Document Set

The penetration test document set is an operational document set that will be maintained as part of the penetration test strategy. There are several discrete elements, each of which may be updated as part of any change penetration test as provided below:

POL00362915

- Business case funding.
- Completed BIA and PIA.
- Project penetration test scope (connections/gateways).
- PCI scope document (if applicable).
- Risks.
- Findings.
- Remediation/tracking plan
- Transfer to operations (outstanding actions, risks, frequency).

4.9 Penetration Test Suppliers – Minimum Requirements

MUST be a member of the UK Government CREST scheme and, as such, provide personnel who maintain one or more of the following certifications in relationship to the scope and type of penetration testing required by Post Office to achieve assurance:

- Offensive Security Certified Professional (OSCP).
- Certified Ethical Hacker (CEH).
- Global Information Assurance Certification (GIAC) Certifications (e.g., GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), or GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)).
- CREST Penetration Testing Certifications.
- Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) certification.

POL00362915

5 Where to go for help

5.1 Additional Policies and Standards

This standard is part of the Cyber Security Policy framework. The full 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 IT Helpdesk

5.3 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

POL00362915

6 Version Control & Approval

6.1 Version Control

Date	Version	Updated by	Change Details
02/05/2018	0.1	IT Security	Changed to the new template for policies Changed to reflect the new Post Office structure First draft
23/05/2018	0.2	IT Security	Updated post peer review
24/05/2018	0.3	IT Security	Updated with further peer review comments
28/05/2018	1.0	IT Security	Final Approved Version
02/12/2021	1.1	Cyber Security	Review with Richard Miller and updated the section 3.4 and 4.5.
17/12/2012	1.1	Cyber Security	Cyber Security Final Approved Version
10/04/2023	1.2	Cyber Compliance	Annual update and review. Wider business input for UCF update required.
25/04/2023	1.3	Cyber Compliance	CSF approval for publication.

6.2 Standard Approval

Standard Owner: Chief Information Security Officer

Standard Author: Ehtsham Ali

Approved by CSF: 25/04/2023

Next review: 25/04/2024