POL00397485

Post Office Internal

Penetration Testing Policy (S7)

1 Purpose

This policy defines the controls required to reduce the risks associated with the management of Security Health Checks.

2 Policy

2.1 Scope

All roles authorised to manage Security Health Checks on behalf of Post Office Limited must comply with this policy.

2.2 Accountabilities

The Head of Security is responsible for the provision of funding for Security Health Checks on enterprise systems / applications and ensuring that tests results are validated and addressed through improvement programmes.

Business Units are responsible for the provision of funding for Security Health Checks on business-specific systems / applications and ensuring that tests results are validated and addressed through improvement programmes.

System / Application Owners are responsible for assessing the requirement for Security Health Checks and responding to test results by implementing improvement programmes.

Security Health Check Managers are responsible for the management of external Security Health Check Teams and liaison with IT Service Providers to ensure that tests are conducted in accordance with this policy.

2.3 Requirement for Security Health Checks

Security Health Checks, sometimes referred to as 'Ethical Hacking', are conducted to provide assurance to stakeholders that critical systems and applications are adequately protected against violations of confidentiality, integrity and availability.

A Security Health Check aims to attack selected resources using similar techniques that would be used by those intending harm. However, the tests are conducted in a controlled manner in order to expose potential threats and build an action plan to close the system to intruders.

2.4 Security Health Check Funding

Post Office Limited Operations will take a holistic view and fund Security Health Checks on systems and applications that are strategic to the enterprise.

Business units will fund Security Health Checks on systems and applications that are strategic to the unit.

2.5 Identification of Targets and Prioritisation of Testing

There are three main reasons for undertaking Security Health Checks:

- Exceptional Changes, where events outside the normal running of the business change the information security environment.

POL00397485

- Formally identified risk, where a formal programme has identified that information may be at risk.
- Life Cycle Changes, where normal testing programmes indicate that a system may still be vulnerable or new methods of attack have been developed.

Priority should be given to those systems whose impact on the business is greatest.

2.6 Critical Systems

No critical system may be declared exempt from a Security Health Check because these are principal targets.

2.7 Types of Testing

Production systems should always be used for testing, unless the nature of the test itself is destructive.

Destructive Tests should only be undertaken where there is a specific need to so do.

Tests should normally be 'informed', with the maximum amount of information given to the testing team.

Tests should normally be 'internal', allowing the testing team to bypass any perimeter defences.

2.8 Employment of Test Teams

Post Office Limited does not undertake Security Health Checks itself. Specialist teams must be employed to undertake testing.

The team must however be managed by Post Office Limited, with a Test Manager assigned for the duration of the project.

2.9 Selection of Test Teams

Organisations used to conduct Security Health Checks for Post Office Limited must be on the approved list of suppliers.

Select only reputable organisations with established track records that are registered with the Government to perform ethical hacking.

Employees of these organisations must be vetted to appropriate government security levels. Post Office Limited does not use organisations known to employ "ex-hackers".

Individual members of the Security Health Check team must be agreed by the Test Manager prior to the testing being carried out.

2.10 Contractual Requirements

2.10.1 Non-Disclosure

A non-disclosure form must be signed by a representative of any organisation bidding to undertake the Security Health Check.

2.10.2 Indemnity

Where direct damage to property is caused by the negligence of either contractual party during the project, then the party shall make good any such damage caused. The Security Health Check Organisation shall indemnify Post Office Limited against all claims demands, costs, charges and

POL00397485

expenses arising from or incurred by any infringement of copyright, patent or other title in respect of materials and delivered software or any part thereof.

The Security Health Check Organisation shall indemnify Post Office Limited against all claims demands, costs, charges and expenses arising from or incurred by any infringement of copyright, patent or other title in respect of materials and delivered software or any part thereof.

2.10.3 Confidentiality

All CONFIDENTIAL information acquired during the course of testing must be stored in a secure manner as described by the S4 Information Classification Policy

All information acquired must only be used solely for the purpose of completing the project, unless required to do otherwise for law enforcement purposes.

2.11 Organisation

The Security Health Check team will be managed by a Test Manager assigned by Post Office Limited. The Test Manager will be responsible to the project sponsor and system owner for carrying out the tests and liaising with other parts of Post Office Limited affected by the tests.

2.11.1 Terms of Reference

Terms of Reference must be produced by Post Office Limited's Test Manager for the Security Health Check team. These will include the objectives, high level scope, method, testing procedure, deliverables, organisation, timeframes and costs.

2.11.2 Test Scope

The Test Manager must agree the scope of testing with the Security Health Check team prior to commencing the test. This will detail the types of test being undertaken.

2.11.3 Emergency Cessation

The Test Manager will ensure that there is the capability to stop testing immediately should a crisis arise. The test may be postponed or cancelled completely.

Cessation of Testing, with minimal disruption and costs, must form part of the contract with the selected supplier.

The Test Manager is responsible for justifying the reason for ceasing testing to the project sponsor and system owner.

2.11.4 Audit Log

A full audit log of testing activities must be maintained in order:

- to identify which areas have been tested so that future tests do not cover the same areas unless there is a valid reason for doing so;
- to exonerate all parties from criminal proceedings should any fraudulent activity be uncovered;
- to expand on recommendations from the report so that weaknesses can be quickly and easily corrected.
- to enable re-testing, if required

POL00397485

- that further similar weaknesses can be identified in other comparable systems by Post Office Limited staff without the need for a specialist team

It is the responsibility of the Test Manager to ensure that the audit log is maintained.

2.11.5 Communication

All communications relating to Security Health Check activities must be treated as CONFIDENTIAL - see S4 Information Classification Policy

Communication to those not involved in the test should be minimised. Safeguards, however, need to be in place to inhibit unwarranted activity potentially caused by testing.

It is the responsibility of the Test Manager to ensure that minimal but effective communication is in place.

2.11.6 Reporting Requirements

A full report must be generated containing a description of all the weaknesses found and suggested measures for either removing them, or minimising the risk.

The report must be treated as CONFIDENTIAL and issued to:

- Head of Information Security or representative
- Owner of target system
- Security Health Check Manager

Reports may be distributed to other roles in Post Office Limited on a strict need to know basis with the agreement of the owner of the target system and under the control of the Test Manager

Major findings, conclusions and recommendations will be presented to:

Key Information Security managers and staff

Business Managers using the target system and any business employees required to undertake remedial action

Technical Managers supporting the target system and any technical staff required to undertake remedial action

2.11.7 Actions on completion

Upon completion of the Security Health Check, the owner of the target system is responsible for ensuring that recommended actions are implemented.

2.12 Re-testing

Upon completion of the Security Health Check, either re-testing or a post implementation review will be recommended to ensure that the target system is secure. It is the responsibility of the system owner to ensure that the appropriate action is taken.

3 Links to other reference material

ISO/IEC 2700117799: 2000 Part 1: Code of Practice for Information Security Management ©

S4 Information Classification Policy

POL00397485

4 Document details

Owner:	Head of Security (POL)	**Enquiry point:**	Sue Lowther Mobile: GRO
Version:	3	**Effective from:**	Current
Last updated:	January 2010	**Review date:**	January 2011