POL00362917

Cyber Security Guideline

Secure Configuration Guideline

Version – V2.2

POL00362917

POL00362917

1 Overview

1.1 Introduction by the Guideline 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 Secure Configuration Guideline is to:

- Provide a statement of intent describing how devices (including virtual instances) should be configured and managed in accordance with Cyber and Information Security requirements and industry best practices.
- Identify the scope of systems to which the Guideline applies.
- Define key processes that support the implementation of this Guideline.

1.3 Core Principles

Alignment with this Guideline will ensure that the following principles are met:

- Physical Installations will be carried out in accordance with best industry practice.
- Security baseline hardening will be applied
- Following best practice will limit the risk of vulnerabilities being introduced into the Post Office Environment

1.4 Application

This Guideline applies to the secure management of Post Office's servers, desktops and mobile devices.

POL00362917

2 Policy Framework

2.1 Policy Framework

This guideline 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 the Cyber Security Policy set 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 the POL policies and standards or have their own equivalent policies/standards

POL00362917

3 Secure Configuration

3.1 Servers

All assets used to deliver services to Post Office should follow industry recognised build standards, physical installation should be carried out in accordance with best industry practice. (e.g. Center for Internet Security (CIS) benchmarks, minimum NCSC best practice for a high risk system). Cyber Security should have agreed to the baseline standards being used. The build standard should recognise the sensitivity of data to be held or transmitted, and where that asset sits within the Post Office network.

Security controls set by the service supplier should be robustly implemented across the platform. Where possible the supplier should technically enforce a minimal set of security critical policies on the device.

Changing manufacturer or vendor defaults before installing a system on the network including, but not limited to, passwords, SNMP community strings and deleting unnecessary accounts is mandatory. Guest and other anonymous accounts should be removed, or disabled if removal is not possible. Operating systems shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and HIPS . All unnecessary services and protocols should be disabled.

The auto-run feature should be disabled for all drives.

Secure versions of protocols and services should be used at all times; insecure alternatives should be disabled.

File system integrity checking should be configured to run on all critical files during system start-up.

Network devices should authenticate all Time synchronisation technology (NTP) messages received from NTP servers and peers. NTP should be used to synchronise all critical server's clocks and times. The following should be implemented for acquiring, distributing, and storing time:

- Time settings should be received from industry-accepted Tier 1 time sources.
- All systems should have the correct and consistent time.

Time data should be protected.

All SNMP community strings should be read only

All services should run in the context of a system account and not in that of an interactive user.

The system should implement media and device controls to prevent unauthorised access to Import/Export media and devices (including USB)

3.2 Windows Specific Requirements

Windows based Servers should join an Active Directory domain where the standard GPOs are applied. Non domain attached servers are not permitted.

POL00362917

Windows servers in zones close to or at the outside of Post Office Data Network should not have direct access to AD through the firewall. Firewalls at the perimeter and on the internal network should be used where there is a requirement to segregate internal network resources.

3.3 Securing Server Software

All system components and software should be protected from known vulnerabilities by having the latest manufacturer supplied security patches installed.

A full assessment of all security patches and vulnerabilities should be undertaken when they are released and implementation undertaken based on an assessment of the risk to the platform (please see the Patch Management Standard for further details).

Remove any unwanted services that may have become available following the software install. (e.g. HTTP, IRC, SMTP etc.).

Remove all default user accounts created by the software installation and test scripts, databases, sample content and other executables from the install directory.

Remove all non-required compilers.

3.4 Server Administration

An asset inventory should be maintained containing records of all servers (hardware, software, and data).

Highly privileged and administrative accounts should be limited to a group of approved individuals only. A log should be maintained to record who has been given highly privileged and/or administrative accounts and the log should be reviewed every six months for accuracy. Post Office will perform regular reviews of the logs to ensure that access is being managed appropriately. Assignment of privileges should be based on individual personnel's job classification, function and clear definitions of user roles, based on least privilege, should be developed. Evidence of the access approval should be maintained.

Service accounts should only be assigned relevant permissions to run the described service(s) they require. User accounts will never be used for server based functionality.

Encrypt all non-console administrative access using strong cryptography according to Post Office Encryption Standard.

Access and usage privileges for all removable media and external drives should be restricted to administrators who are responsible for server maintenance.

3.5 Desktops and Laptops

All assets used to deliver services to Post Office should follow industry recognised build standards, physical installation should be carried out in accordance with best industry practice (e.g. CIS benchmarks, minimum NCSC best practice).

Account Lockout for standard users after 5 invalid logon attempts and privilege account after 3 invalid logon attempts.

POL00362917

The use of removable storage media should be controlled in accordance with business need and appropriate protection (e.g. cryptography) applied (please see the Encryption Standard and the Remote Access Standard for further information)

All desktops and laptops that are attached to Post Office data networks should be running anti-malware software that is updated regularly (please see the Threat Prevention Standard for further information).

Whole disk encryption should be enforced, and all Post Office data should be encrypted on all assets where not owned or leased by Post Office.

Desktops and laptops should automatically lock themselves after being idle for 15 minutes and require a password to unlock.

User accounts should be restricted from modifying operating system files and system registry settings.

Only approved software can be installed on Post Office devices and the approved software can only be installed by the users who have been assigned the privileges to do so.

If approved software has to be manually installed instead of being deployed using a fully tested package, an install guide has to be created to ensure that the software is installed in a consistent manner and devices are checked for any vulnerabilities that may have been introduced as part of the install such as:

- unwanted services that may have become available that need to be removed. (e.g. HTTP, IRC, SMTP etc.)
- any unwanted default user accounts
- test scripts
- databases
- sample content
- any other executables from the install directory that would otherwise leave the device vulnerable

All non-required compilers should be removed.

Auto-run should be disabled

POL00362917

4 Where to go for help

4.1 Additional Policies

This guideline is one of a set of policies. The full set of policies 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[redacted] GRO

POL00362917

5 Version Control & Approval

5.1 Version Control

Date	Version	Updated by	Change Details
23/01/2020	1.0	IT Security	Changed to the new template for Guidelines
12/06/2020	1.0	Cyber Security	Approved by ISC
29/07/2021	1.1	Cyber Compliance	Final draft for approval
02/08/2021	2.0	Cyber Compliance	Approved by ISC
04/04/2023	2.1	Cyber Compliance	Updated the name from Platform Security to Secure Configuration and align to the UCF
25/04/2023	2.2	Cyber Compliance	CSF approval for publication.

5.2 Standard Approval

Guideline Owner: Chief Information Security Officer

Guideline Author: Ehtsham Ali

Approved by CSF: 25/04/2023

Next review: 25/04/2024