POL00362913

Cyber Security Guideline

Network Security Guideline

Version – V2.2

POL00362913

POL00362913

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 this guideline is to provide further detail to support the Network Security Standard for data network components. The resulting configuration will assist in the protection of Post Office's assets and information from unauthorised access and external threats.

1.3 Core Principles

This Guideline will aid in ensuring that the following principles are met:

- Technical and procedural standards are defined and implemented for secure and effective deployment and maintenance of data network services in support of business objectives.
- The configuration of data network components does not expose Post Office to security threats.
- Compliance to the business requirements and items which are subject to legal and regulatory requirements, including specific control requirements for the handling of Payment Card Industry Data Security Standard (PCI-DSS).

1.4 Application

This Guideline applies to all Post Office staff, including third party suppliers providing services to, for, or on behalf of Post Office, and aligns to the requirements of the Cyber Security Policy.

This Guideline applies to the secure management of Post Office's data network, which spans both internal and external boundaries, dataflow, legal implication, monitoring, and protection.

This guideline is applicable to all data networks including branch, corporate, and data centre networks. All suppliers responsible for designing, deploying, managing and hosting Post Office's data network should comply with this standard.

This standard is designed to be universally applied to all data network devices and is independent of:

- Hardware or Software platform.
- Hardware or Software function.

POL00362913

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 this guideline 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.

POL00362913

3 Network Design and Architecture

When considering network design and architecture the following controls should be reviewed and applied if applicable:

- Network should support consistent naming conventions and addressing structures.
- Security levels, domains and/or zones should be implemented to provide appropriate security to the information assets in line with their classification.
- Deployment of security and access control mechanisms to segregate networks into logical domains
- Appropriate perimeter security measures (boundary controls) should be applied, to eliminate direct connections between internal devices and external networks
- Filtering of network traffic between internal and external networks, so that only explicitly defined network traffic is allowed.
- Test systems should be deployed in separate logical domains to production systems. Firewall(s) should be used to segregate test, development and production environments
- Only explicitly allowed traffic is permitted to traverse network boundaries. Securing the confidentiality and integrity of information where internal network links are carried over network infrastructure not controlled by the Post Office (public networks), for example by using Virtual Private Networks (VPN)
- Network design should support secure dynamic routing protocols that allow rapid re-routing around failed network components.
- Networks should be designed in a way that prevents security mechanisms from being bypassed.
- Networks should be designed in a way that minimises single point of failure.
- Networks should comply with statutory and industry regulations.
- All outbound access to Internet web sites and web services should pass through an application level proxy (Web proxy).
- Web traffic originating from external data networks should pass through a reverse proxy and Web application firewall, after it has been decrypted by SSL gateway. A firewall should be installed at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.
- Perimeter firewalls should be installed between any wireless data networks and the cardholder data environment (CDE). These firewalls should be configured to deny or control any traffic from the wireless environment into CDE.
- Terminating points for Site to Site VPNs and VPNs for remote access should be located in a DMZ.
- IDS/IPS should be used in the DMZ environment or any critical domain.

3.1 Minimum document set

Accurate network diagrams should be produced and maintained and reviewed annually for each Post Office IT network, together with a master network diagram showing interconnections between Post Office IT networks and external connections.

Where high risk or personally identifiable information (PII) is processed, documentation should be produced and maintained detailing data-flow.

Diagrams, showing the flow of any personal information and cardholder data, and the devices it is exposed to, including any connections to third-party infrastructure

POL00362913

3.2 Network Reliability

The following controls should be applied:

- Maintenance of all hardware platforms and software running on them at current, supported and replaceable version levels
- Appropriate protection of all network equipment against natural hazards and power failure.
- Network capacity and scalability considerations as part of the assessment prior to the introduction of new technology systems
- Appropriate protection against capacity saturation (denial of service) attacks;
- Establishment, where appropriate, of fallback arrangements for each network service.

3.3 Network Management and Operation

The following controls should be applied:

- Devices should not be connected to more than one network segment, or to an internal Post Office network and external network at the same time, unless the device is part of the network boundary protection (such as a proxy server or firewall);
- The Post Office IT Change Control Process should be used for all changes to network design, including firewall rules;
- Network devices should be patched in accordance with the Post Office Patch Management Standard;
- All cables and patching sockets should be labelled;
- Patching documentation should be maintained detailing where all cabling is installed
- Provision of network performance monitoring and alerting in real-time.

3.4 Authentication

- Users will only be granted access to the device after successful authentication.
- All users should use their unique ID to authenticate to the data network devices.
- All vendor supplied default passwords should be changed to an alternative strong password before installing a system or device on the data network as per the Platform Security Standard
- All users should use a strong password as per the Access Control Security Standard.
- User access should be configured according to the principle of least privilege.
- Where technically possible, a central TACACS+/Radius system should be used for authentication to data network devices.
- In combination with centralised user authentication, command logging should be enabled to provide audit trails.
- Access to data network devices for the purposes of management should occur via encrypted connection, using the most secure method as per the Encryption Standard.
- All unsecure access methods (i.e. Telnet, HTTP, SSHv1) should be disabled.
- Virtual access (SSH) to a device should be limited to management systems only to decrease the chance of potential attacks.

POL00362913

- Connections to data network devices should be configured with an idle timeout of no longer than 30 minutes where possible. Where 30 minutes or less is not possible, timeout should be set to lowest timeout available.
- Any credentials, passwords, authentication keys or community strings should be stored in encrypted or hash formats as per the Encryption Standard.
- Public and Private SNMP Community Strings should be changed prior to a data network device being installed on the data network. No default community strings are permitted.
- SNMPv3 should be used in preference to SNMPv2 wherever possible for managing and monitoring of data network devices to guarantee data integrity and security.
- SNMP Read-Only access should be used where possible.
- An Access List should be created to ensure only authorised management hosts can access SNMP-enabled devices. This list should be reviewed annually to ensure accuracy.
- SNMP traps should be configured to send a trap to the appropriate host in the event of an authentication failure for the community string.

3.5 Access Control

- All devices should be operated based on the principle of 'least privilege'.
- Where applicable, data network infrastructure should only be accessed from internal addresses.
- Warning banners should be present on all interactive access to data network devices to warn of unauthorised access being prohibited.
- Any modem or data network device that gives access to the console port should be secured using appropriate physical or logical controls.
- Remote maintenance ports should only be enabled during support windows.
- Only 'in use' physical ports should be activated on the LAN. Unused ports should be disabled to prevent unauthorised access to the data network.
- Egress filters should be used where risk warrants such protection.
- All Internet accessible servers should always be placed in a DMZ.
- Anti-spoofing filters/capabilities should be enabled where possible.
- Control of physical access to critical networking areas and equipment in accordance with ISO27001 Physical Security or similar best practice.

3.6 NAC Access Control

If NAC Access control is in place it should:

- Deploy an automated asset inventory discovery tool and maintain an asset inventory of systems connected to Post Office's data networks.
- Maintain an asset inventory of all systems connected to the data network and the data network devices themselves.
- Deploy NAC such that if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.
- If Post Office request it, the NAC service should manage a list of authorised software that is required for each type of system, including servers, workstations and laptops of various kinds and uses. This list should be tied to file integrity checking software to validate that the software has not been modified. The service

POL00362913

provider should perform regular scanning for unauthorised software and generate alerts when it is discovered on a system.

3.7 Device Configuration

Minimum controls for device configuration:

- All data network equipment should utilise a central time source where technically feasible.
- Any changes to data network devices should follow the agreed change management processes and include backup of the device configuration for significant changes.
- A complete list of all data network devices should be maintained in a Configuration Management Database (CMDB), or equivalent solution.
- Security updates should be issued by the enterprise and the enterprise should remotely validate the patch level of the device estate.
- All data network devices should maintain appropriate security levels through the deployment of security patches as per Post Office Patch Management Standard
- Software versions should be consistent across devices of the same classification unless prevented by technical constraints.
- Security patches should be deployed following the Post Office Patch Management Standard.
- Reviews of major and minor software releases should occur every 6 months and decisions regarding implementations should be documented.
- Configuration of all devices with the minimum services necessary
- Disabling, where possible, unauthenticated access from the network to internal information about network devices (such as version numbers)
- Configuration of all devices in line with the Platform Security standard

3.8 Firewalls

- All firewall rules should be documented to show their purpose, and be implemented under appropriate change control.
- Default firewall policy should be to Deny All on all ports, both inbound and outbound. Access should be granted only on an as-needed business basis using ingress and egress filtering.
- The use of 'Any Source and Any Destination' rules (commonly known as 'Any-Any') is prohibited.
- All ports, connections, objects, rules, and IP addresses should be documented for audit trail purpose. Firewall rulesets should comply with all applicable security policies.
- Rules should be audited regularly in order to ensure they remain appropriate and necessary.
- VPN termination points should be configured with acceptable encryption algorithms and key lengths as specified in the Encryption Standard.

3.9 Routers and Switches

- Router and switch configuration files should be secured and synchronised.

POL00362913

- Configuration standards should be developed in line with industry accepted hardening standards. These standards should be agreed with Cyber Security and be in line with the Post Office Platform Security Standard
- Routers (including data network components that perform routing) should be configured to prevent unauthorised updates.
- Access to console ports, auxiliary ports and virtual terminal ports should be restricted.
- Unnecessary data network services, ports, protocols and ports should be disabled.
- Data network traffic in and out of the cardholder data environment (CDE) should only be routed to and from destinations authorised and approved by Cyber Security
- IP masquerading should be implemented to prevent internal addresses from being translated and revealed on the Internet using Network Address Translation (NAT) and Port Address Translation (PAT) mechanisms.
- IP Source routing should be disabled on all routers.

3.10 Vulnerability Management

Vulnerabilities, including performance of scans and penetration tests, should be managed in accordance with the Penetration Testing and Vulnerability Scanning Standard.

3.11 Logging & Monitoring

- Data network security controls will be configured to send security logs and audit trails of management activities to a centralised SIEM solution, which will manage the logs as per the Logging and Monitoring standard.
- The internal network configuration should be hidden or obfuscated from external users. Network traffic will be limited to specific IP application protocols as required for the business
- IP address white listing should be used for all outbound traffic and should be utilised by service providers where the sole connectivity is to Post Office networks
- Boundary firewalls should be configured to prevent LAN management access to the System from external connections
- Network IDS and IPS should be installed on all boundary networks or network zones to monitor and prevent suspicious traffic
- Packet filtering should be carried out at the perimeter to filter out unwanted packets and reduce the workload for externally facing firewalls.
- Suspicious or infected traffic should be quarantined for further analysis.
- Analyse all traffic exiting the network to perform data leakage prevention preventing access to social data sharing sites and traffic entering the network to detect and block possible malicious or high risk content
- All connections should pass through a common aggregation point.
- Outbound Connections should always be initiated from the more secure domain into the less secure domain
- Blacklists should be used as an additional control to prevent access to obviously bad sites, but should not be relied upon exclusively as it is impractical to blacklist every bad site on the Internet
- Servers and appliances should not have direct Internet access unless there is a specific business need that has been approved by the relevant accreditor
- Remote device connections should be appropriately identified and authenticated by the perimeter network before being allowed access to internal resources

POL00362913

- Ensure that any Internet facing services are protected by the perimeter network, to ensure only authorised secure access is allowed to the internal network.
- Where practical, external connections should include some form for protocol break or inspection (depending on threat). This could include be as simple as passing connections through a proxy or may be more in depth, depending on specific threats
- Encrypted tunnels (such as SSL web browsing) should not be allowed to the untrusted network without being broken and inspected at the gateway.
- The gateway should inspect traffic and attempt to detect known malware command and control traffic
- The firewalls should only permit ports which are required for the gateway to operate
- Connection to trusted site should be appropriately authenticated and encrypted using strong credential such as mutual SSL certificated issued by know trusted certificate authorities
- All management traffic should be separated from data traffic; logical and physical separation techniques are both acceptable
- Management access network routes should not create bypasses around existing security devices
- Please also see the Post Office Logging and Monitoring Standard

POL00362913

4 Where to go for help

4.1 Additional Policies

This guideline is part of the Cyber Security Policy framework. The full set can be found at:

IRRELEVANT

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 **GRO**

POL00362913

5 Version Control and Approval

5.1 Version Control

Date	Version	Updated by	Change Details
22/01/20	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 version by ISC
23/11/2022	2.1	Cyber Compliance	Annual Review and to updated to the UCF controls
25/04/2023	2.2	Cyber Compliance	CSF approval for publication

5.2 Guideline Approval

Standard Owner: Chief Information Security Officer
Standard Author: Hazel Freeman
Approved by Owner: 25/04/2022
Next review: 25/04/2023