POL00362908

Cyber Security Standard

Bring Your Own Device (BYOD) Standard

Version – V3.3

POL00362908

POL00362908

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

This Cyber Security Standard covers the use of non-Post Office supplied devices for accessing Post Office systems and data (popularly known as "Bring Your Own Device", or BYOD).

1.3 Core Principles

To enable user-owned devices to be approved and used in line with Post Office business requirements when accessing Post Office systems and data, ensuring critical and sensitive business information is protected appropriately from misuse or loss.

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.

POL00362908

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.

POL00362908

3 Supported Devices

The Post Office BYOD solution supports the following devices running a current manufacturer supported operating system:

- Any Windows laptop
- Any Apple laptop running macOS
- Any Smart Phone running Android or iOS
- Any tablet running Linux, Android or iOS

The following BYOD's are specifically excluded from support and not permitted to access POL systems or data:

- Windows Mobile (except company issued phones)
- Versions of Kali Linux
- Proprietary mobile operating systems
- "Jail Broken" or "Rooted" devices

All BYOD's must be approved and utilise the method provided to access Post Office systems and data. Post Office will accept no liability for loss, damage or corruption of BYOD's.

Access to Post Office Systems from a BYOD will require the use of a second authentication factor (e.g. hardware or software token; text message-based; or message to an independent device)

Each BYOD must only be used by the respective authorised individual who will remain liable for Post Office information stored, processed or transmitted on that device. No shared usage of BYOD's or credentials is permitted.

In the event that anyone partaking in the BYOD scheme:

- leaves the Post Office
- has the device stolen
- sells the device
- submits the device for repair
- discards the device

All Post Office Data applications and any key/certificate/authentication data must be deleted. If you are unable to do this or in the event of a stolen device, please see 4.4 Incident Management.

POL00362908

4 Device Management

All BYOD's will be required to implement a level of security which will be verified by the

Management Solution.

An "isolated environment" will be implemented on BYOD's and specific controls will be enforced which will be under the governance of the POL Mobile Device Management (MDM) solution. Any data, applications or settings which are stored in that environment will be managed as if on a POL provided device; and may be audited, accessed or deleted at any time as required by business needs. Connection to Post Office resources is contingent on the user accepting that control of those privileges remains with Post Office and any such resources or access may be removed from the device at any time.

Specific training for users of the service to be provided and all users will be required to undertake that training including regular refresh.

Controls commensurate with the business risk of using BYOD's will be implemented through technical and procedural measures.

4.1 Data Network Connection

BYOD's must only connect via Internet facing systems or those provided by Post Office specifically for that purpose.

The following are specifically prohibited:

- Direct connection to any Post Office internal data networks.
- Connection to any Remote Access Service associated with Post Office internal data networks.
- Connection to Post Office Cardholder Data Environment (AWS-CDE).

4.2 Configuration

Device configuration will be verified to ensure it complies with minimum levels and may require installation or software, changes to configuration and other controls. Controls that will be assessed or enforced include:

- Use of an identification mechanism, e.g. digital certificate/device identification reference, unique to that device and not transferrable.
- Implementation of current malware protection where appropriate
- Application of relevant security updates.
- Protection of logical access to the data/application by use of a strong password/long PIN
- Encryption of POL data stored locally on the device.
- All BYOD's will be registered in a Post Office management system and must regularly connect to that system to verify their configuration.
- Install personal firewall on employee-owned computer with direct connectivity to the internet, which are used to access the Post Office network.
- Automatic disconnect of session for remote-access technology fifteen minutes inactivity.

POL00362908

4.3 Auditing

Use of BYOD's to access POL systems will be recorded on a central Post Office database. That use will be subject to auditing, logging and monitoring including:

- Activity within the application on the device
- Connectivity to the management solution
- Connection to the access solution

BYOD's that have not connected to the central MDM system for more than a month, will trigger verification with the User, to determine if the BYOD access is still appropriate.

4.4 Incident Management

In the event of the loss of a BYOD which has been used to access Post Office resources, the user must immediately inform the Post Office IT Helpdesk and Cyber Security so that further access may be blocked and any Post Office information removed.

In case of a security incident involving BYOD's, Post Office may ask the user to submit their device to forensic examination where it is believed to contain, or to have contained, data or log files necessary investigation or control purposes.

Forensic investigations will always comply with the Incident Management process, and be in line with related policies and legislation.

POL00362908

5 Data

All Post Office Data must be processed according to the Acceptable Use Standard. Participants agree to removal of all information relating to Post Office from their Device, on exit, or on demand.

BYOD users must keep information and documentation resulting from private activities, separate from business data on the personal device in separate directories, clearly named (e.g. "Private" or "Personal" versus "Post Office"). Any data held in a dedicated Post Office area is liable to be deleted at any time at the discretion of Post Office.

Post Office data must never be uploaded to any public cloud infrastructure, including backups of Post Office data.

POL00362908

6 Where to go for help

6.1 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

6.2 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

6.3 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

POL00362908

7 Version Control & Approval

7.1 Version Control

Date	Version	Updated by	Change Details
03/09/2015	0.1	IPA	Initial draft release
29/07/2016	1.0	IPA	Final version
21/04/2017	1.1	IT Security	Revision to take into account organisational changes. Validation against revised technical strategy and changes to accommodate
05/02/2018	2.1	IT Security	Reviewed - GDPR
06/02/2018	2.2	IPA & IT Security	Changed to the new template for policies Changed to reflect the new Post Office structure Minor editorial changes at annual review
30/05/2018	3.0	IT Security	Updated post peer review and approved
31/01/2022	3.1	Cyber Security Compliance	Minor updates apply to sections 3 and 4.
10/04/2023	3.2	Cyber Compliance	Annual update and review. Wider business input for UCF update required.
25/04/2023	3.2	Cyber Compliance	CSF approval for publication

7.2 Standard Approval

Standard Owner: Chief Information Security Officer
Standard Author: Ehtsham Ali
Approved by CSF: 25/04/2023
Next review: 25/04/2024