POL00362906

Cyber Security Standard

Access Control Standard

Version – V3.2

POL00362906

POL00362906

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

There are various levels of access required to perform tasks in accordance with a user's defined role.

To reduce risk, role-based profiles must be assigned based on the appropriate permissions and assignments associated with the task and/or function to be performed.

In practice, managing user credentials is a significant part of any facility, system or application administrator's role and the purpose of this document is to state the minimum controls to ensure appropriate access to the facilities, data network infrastructure and information resources is granted to authorised users/personnel only.

1.3 Standard Guidance

Access control ensures that actions or operations a user can perform on Post Office systems and in physical locations are limited, seeking to prevent activities which could lead to breach of security.

Users should only be granted access to information assets and facilities on a 'need-to-know' and 'need-to-have' basis (principle of least privilege).

Users should only be granted the minimum access and privileges required to perform their duties.

Each assigned user credential should uniquely identify the user and must conform to the Post Office naming standard (e.g. first and last name), or an appropriate naming structure. User credentials must not give any indication of the user's access rights.

Security of system administration user credentials and their passwords is the responsibility of the Service Provider, (SP) and must adhere to the relevant controls in this standard, except for where this is not technically feasible, or if the control requirement is not part of the service provided, an exception must be raised and approved.

Data Owner(s) (DO) must regularly review, (every 6 months for POL Crown Jewel systems) the user Access Control List (ACL) including the roles assigned to information assets they manage as the Information Owner, if any access rights need to be amended trail and up-to-date record of these reviews must be maintained.

System Administrator accounts must be reviewed on a regular basis (monthly for POL Crown Jewel systems) to ensure access and account privileges remain appropriate to the specific job function, role or employment status of the user, these reviews must be performed by an independent third party with appropriate authority who does not have

POL00362906

Administrator access to the system being reviewed. An audit trail and up-to-date record of these reviews must be maintained.

Access will be revoked for user credentials that no longer require access in order to maintain the confidentiality, integrity and availability of information to authorised users only.

1.4 Application

This standard applies to all Post Office staff and Third-Party organisation's who have access to Post Office data especially those with elevated rights to Post Office data.

This Access Control Standard is amended from time to time, and 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 and Information Security Policy.

POL00362906

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.

POL00362906

3 Minimum Controls

The table below sets out the minimum control standards.

Control Ref	Control Objective	Control Guidelines
PHT0453 CTRL0020636	Establish, implement, and maintain an access control program.	Include instructions to change authenticators as often as necessary in the access control program. Include guidance for how users should protect their authentication credentials in the access control program. Include guidance on selecting authentication credentials in the access control program. Establish, implement, and maintain access control policies. Disseminate and communicate the access control policies to all interested personnel and affected parties.
PHT0459 CTRL0020637	Establish, implement, and maintain an access rights management plan.	Inventory all user accounts. The organisation has a defined and implemented access rights management plan as part of their user access control policy. An audit trail of access to information classified as highly sensitive is maintained by the relevant stakeholder.
PHT0461	Identify information system users.	Review user accounts. Review and update accounts and access rights when notified of personnel status changes.

POL00362906

Control Ref	Control Objective	Control Guidelines
PHT0464 CTRL0020582	Control access rights to organizational assets.	Define roles for information systems. Define access needs for each role assigned to an information system. Define access needs for each system component of an information system. Define the level of privilege required for each system component of an information system. The organisation has a defined and implemented User Access Control Standard, which includes third parties. Evidence is retained that access is provided on completion of appropriate authorisation and procedural documentation before access is granted. Access provisioned is in line with the user's job role and with that requested.
PHT0469 CTRL0020603	Establish access rights based on least privilege. (every 6 months)	Assign user permissions based on job responsibilities. Assign user privileges after they have management sign off. Separate processing domains to segregate user privileges and enhance information flow control. Maintain user access rights in accordance with business function and process requirements. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles and separation of duties. Privileged accesses on system, database and application level is appropriately restricted and monitored

POL00362906

Control Ref	Control Objective	Control Guidelines
		Separate processes are in place to segregate and manage privileged user accounts. All privileged user accounts and access privileges are reviewed at least quarterly, to ensure access privileges remain appropriate
PHT0473	Establish, implement, and maintain lockout procedures or lockout mechanisms to be triggered after a predetermined number of consecutive logon attempts.	See Appendix for details
PHT0474	Enable access control for objects and users on each system.	Include all system components in the access control system. Set access control for objects and users to "deny all" unless explicitly authorized. Enable access control for objects and users to match restrictions set by the system's security classification. Enable role-based access control for objects and users on information systems.
PHT0479	Assign Information System access authorizations if implementing segregation of duties.	Enforce access restrictions for change control. Enforce access restrictions for restricted data. Provide administrators with named accounts for business use.
PHT0482	Perform a risk assessment prior to activating third party access to the organization's critical systems.	Activate third party maintenance accounts and user identifiers, as necessary.
PHT0484	Document actions that can be performed on an information system absent identification and authentication of the user.	Use automatic equipment identification as a method of connection authentication absent an individual's identification and authentication.
PHT0486	Control user privileges.	Review all user privileges, as necessary. Limit the number of privileged user accounts All privileged actions must be attributed to a single individual where this is technically possible.
PHT0488	Establish, implement, and maintain User Access Management procedures.	Establish, implement, and maintain an authority for access authorization list.

POL00362906

Control Ref	Control Objective	Control Guidelines
		Review and approve logical access to all assets based upon organizational policies.
PHT0491	Control the addition and modification of user identifiers, user credentials, or other authenticators.	Assign roles and responsibilities for administering user account management. Refrain from allowing user access to identifiers and authenticators used by applications.
PHT0494	Remove inactive user accounts, as necessary.	Access rights for leavers must be removed within 24 hours of their last day. Access rights for high risk staff must be removed immediately on notification of termination or last day. See Appendix
PHT0495	Terminate user accounts when notified that an individual is terminated.	Terminate access rights when notified that an individual is terminated. Revoke asset access when an individual is terminated.
PHT0498	Disseminate and communicate the password policies and password procedures to all users who have access to restricted data or restricted information.	See Appendix
PHT0500	Establish, implement, and maintain access control procedures.	Disseminate and communicate the access control procedures to all interested personnel and affected parties.
PHT0502	Establish, implement, and maintain an identification and authentication policy.	Establish, implement, and maintain identification and authentication procedures.
PHT0504 CTRL0020686	Include digital identification procedures in the access control program.	Employ unique identifiers. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable. Uniquely identify all information processing activities by user.
PHT0506	Include instructions to refrain from using previously used authenticators in the access control program.	See Appendix

POL00362906

Control Ref	Control Objective	Control Guidelines
PHT0507	Authenticate user identities before manually resetting an authenticator.	Passwords should not be reset or provided to the user unless the users identity has been challenged, confirmed and approval has been given.
PHT0508	Require proper authentication for user identifiers.	Assign authenticators to user accounts. Assign authentication mechanisms for user account authentication. Refrain from allowing individuals to share authentication mechanisms. Use biometric authentication for identification and authentication, as necessary. All systems must be designed with secure access. Users must access the system by providing an unique user name and password, and where applicable privileged users must use multifactor authentication
PHT0568	Enforce privileged accounts and non-privileged accounts for system access	Limit the number and use of privileged accounts, (minimise privileges for all users). Provide administrators with named accounts for business use. Implement the requirement for a privileged account review which is more frequent than for standard accounts. Monitor all user activities, particularly access to sensitive information and the use of privileged accounts. User credentials must be reviewed on a regular basis to ensure access and account privileges remain appropriate to the specific job function, role or employment status of the user. An up-to-date record of these reviews must be maintained. Roles Matrices must be updated when roles are changed. MFA must be implemented for cloud root accounts

POL00362906

POL00362906

4 Appendix A – Password Requirements

To ensure that passwords are of adequate strength for users, systems, applications, and devices these must meet, to the degree where technically feasible, the following Information Security control requirements:

Description	Control	Rationale
Password Expiration	**90** days	Enforcing a password age will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.
Minimum Length for Standard Users	**8** characters	Enforcing a minimum password length to protect against brute force and dictionary attacks, and increases the efficacy of password-based authentication systems.
Enhanced Length for High Privilege Accounts	**15** characters	Enforcing an enhanced password length for sensitive and critical information assets to protect against brute force and dictionary attacks, and increases the efficacy of password-based authentication systems for a higher-level of security.
Service Accounts	**30** characters	Enforcing an enhanced password length for accounts where regular password change is not feasible to protect against brute force and dictionary attacks, and increases the efficacy of password-based authentication systems for a higher-level of security.
Password Complexity	**3** out 4 character types	Enforcing password complexity requirements using alphanumeric and non-alphanumeric reduces the probability of an attacker determining a valid credential.
Password Complexity (Privilege Accounts)	**4** out 4 character types	Enforcing password complexity requirements using alphanumeric and non-alphanumeric reduces the probability of an attacker determining a valid credential.
Password History	**24** passwords remembered	Enforcing a sufficiently long password history will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential. For example, if an attacker compromises a given credential that is then expired, this control prevents the user from reusing that same compromised credential.

POL00362906

Description	Control	Rationale
Account Lockout for Standard Users	After **3** invalid logon attempts	Enforcing an account lockout threshold will almost eliminated the effectiveness of automated brute force password attacks and improves the security of information resources.
Account Lockout for High Privilege Accounts	After **3** invalid logon attempts	Enforcing an account lockout threshold for sensitive and critical information assets will almost eliminated the effectiveness of automated brute force password attacks and improves the security of information resources.
Account Deactivation	**40 days**	If any account is not being used for 40 consecutive days, it must be deactivated so it cannot be misused.
Lock-Out Duration	**60** minutes	This reduces the probability of an attacker successfully determining a valid credential. Additionally, establishing a reasonable time-out period will prevent an attacker from intentionally locking out all accounts until accounts automatically unlocks after 60 minutes or the Service Desk manually resets the account.
Screensaver	Idle after **15** minutes, password protected	Enabling the screen saver will help prevent an unauthorised user from hijacking the computer if attended or remotely. Release from the locked state must require the user to re-enter their password.
Session Timeout	Idle after **15** minutes, password protected	Enable session timeouts this will prevent an authorised user from hijacking the computer if attended or remotely. User will be required to log back in.

POL00362906

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:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

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

POL00362906

6 Version Control & Approval

6.1 Version Control

Date	Version	Updated by	Change Details
29/05/2018	1.1	IT Security	Changed to the new template for policies Changed to reflect the new Post Office structure Minor editorial changes at annual review
08/06/2018	2.0	IT Security	Final Approved Version
03/11/2018	2.1	IPA	Add timeout for VPN, and minor editorial changes.
10/12/2018	2.2	IPA	More changes as requested by ISC following review of external practices to do with password length and complexity.
10/01/2019	2.3	IPA	Final Approved Version.
04/04/2020	2.4	Cyber Security	Updated to include archer controls, add in 30 character password limit and revert back to 90 day password expiration.
12/06/2020	2.4	Cyber Security	Approved by ISC
28/07/2021	3.0	Cyber Compliance	Final Approved Version
07/11/2022	3.1	Cyber Compliance	Added revised control set aligning with the UCF controls
25/04/2023	3.2	Cyber Compliance	Approval by the CSF for publishing

6.2 Standard Approval

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