POL00362916

IT Security Standards

Remote Access Standard

Version – V1.2

POL00362916

POL00362916

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

The purpose of the Remote Access Standard is to mitigate the risks associated with privileged users accessing POL environments.

1.3 Core Principles

Compliance with this standard will aid in ensuring that the risks associated with working and accessing Post Office information and environments remotely by privileged users will be mitigated.

1.4 Application

This standard relates to all people, systems, networks, and services used to support the Post Office, including those managed, maintained and supported by and on behalf of the Post Office by suppliers, partners and Post Office employees.

POL00362916

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 standard/policy.

POL00362916

3 Minimum Controls

The table below sets out the minimum control standards.

Control Number	Control Detail	Attestation Guidance
PHT0569 CTRL0020584	Control all methods of remote access and teleworking.	Establish, implement, and maintain a remote access and teleworking program. Implement strong controls over remote access by privileged user
PHT0571	Control remote access through a network access control.	To ensure protection against data leakage, unauthorized access, computer virus intrusion, and other major incidents, access to the internal network and utilization of remote access should be in accordance with prior specified procedures
PHT0572	Employ multifactor authentication for remote access to the organization's network.	Use two-factor authentication and strong encryption for remote access. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure
PHT0573	Implement multifactor authentication techniques.	To be ready for cases of passwords leakage, other measures such as multifactor authentication or multilevel authentication may be used together with passwords, in accordance with the content of services used and the properties of related risks
PHT0574	Monitor and evaluate all remote access usage.	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: - Enabled only during the time period needed and disabled when not in use. - Monitored when in use Access to critical systems and networks by external individuals for remote maintenance purposes (e.g., remote diagnosis / testing, software maintenance) should be managed by logging all activity undertaken.

POL00362916

4 Where to go for help

4.1 Additional Policies

This standard is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.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 GRO

POL00362916

5 Version Control

5.1 Version Control

Date	Version	Updated by	Change Details
27/04/2018	0.1	IT Security	Changed to the new template for policies Changed to reflect the new Post Office structure First draft
23/05/2018	0.2	IT Security	Updated post peer review
29/05/2018	1.0	IT security	Final Approved Version
14/04/2023	1.1	Cyber Compliance	Updated to cover remote access only, portable devices are covered by BYOD and AUP standards
25/04/2023	1.2	Cyber Compliance	CSF Approval for publication

5.2 Standard Approval

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