POL00362894

GROUP POLICY

Cyber and Information Security

Version – V3.1

POL00362894

POL00362894

1. Overview

1.1. Introduction by the Standard Owner

Post Office.[1] 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 polides, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

The CIO has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter or ensure that Post Office is protected from all Cyber Security threats.

1.2. Purpose

The purpose of this policy is to detail the minimum IT controls required to reduce the Post Offices exposure to information security threats such as:

- Threats from the internet (cyber threat)
- Threats from internal staff (either malicious or accidental)
- Threats from third parties (either malicious or accidental)

1.3. Core Principles

Compliance with this Group policy will ensure that the following principles are met:

- External suppliers identified and categorised such that a risk-based approach can be facilitated in assessing the supplier's security controls.
- Security arrangements can be negotiated and embedded into service agreements and contracts.
- Security controls can be validated prior to services commencing and on an ongoing basis.
- Termination of third-party relationships can be effectively managed so as not to expose Post Office to additional Risks.
- Undertakes a training and awareness program to ensure employees are aware of the Cyber Security responsibilities, what they should do if they are suspicious, and the potential consequences.
- Decisions taken by management are consistent with the Board's approved strategic objectives and Risk Appetite.
- Every member of staff is responsible for understanding and managing the risks they take on behalf of the Group.

[1] In this Policy "Post Office"" means Post Office Limited and any wholly owned subsidiary - if the policy does not apply to all of these entities then this needs to be articulated in the policy.

POL00362894

1.4. Application

The policy is applicable to all areas within (Post Office Ltd and its subsidiaries[2]) and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Post Office's Risk Appetite

Post Office information assets and systems include, but are not limited to:

- Business environments;
- Business processes;
- Business applications (including those under development);
- Information systems; and
- Networks

In exceptional circumstances, where risk sits outside of the Post Office accepted Risk Appetite a Risk Exception can be granted. For further information in relation to the risk exception process please contact the Risk & Assurance team. CentralRiskTeam[GRO]

Further information in relation to the risk exception process can be found here.

1.5. Legislation

Post Office seek to comply with all relevant UK legislation and regulatory requirements including (but not limited to):

- Data Protection Act (2018).
- Freedom of Information Act (2000).
- Privacy and Electronic Communication Act (2003).
- Regulation of Investigatory Powers Act (RIPA) (2000).
- Copyright, Designs and Patents Act (1988).
- Computer Misuse Act (1990).
- Human Rights Act (1998).
- Terrorism Act (2006).
- Limitation Act (1980).
- Malicious Communication Act 1988).
- Digital Economy Act (2017).
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations (2011).
- Counter-Terrorism and Security Act (2015).

1.6. Industry Guidance

Post Office is a member of the Information Security Forum (ISF) which is used to provide input to all cyber security activity as well as liaising with the National Cyber Security Centre (NCSC) for information and guidance.

[2] Post Office Limited is wholly owned by the Department for Business, Energy and Industrial Strategy (BEIS). It 's business consists of the core products and services provided by Post Office Group (mails, government services (including identity & licences) and retail), as well as selling the services of Group Companies and joint ventures (Post Office Insurance, First Rate Exchange Services Limited and Payzone Bill Payments Limited).

POL00362894

1.7. The Risk

The main risks that face Post Office from a Cyber perspective (and that are addressed by the controls specified in this document) are:

- Threats from the internet (cyber threat)
- Threats from internal staff (either malicious or accidental)
- Threats from third parties (either malicious or accidental) define the risks and types of risk that this policy is intended to address)

POL00362894

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which Post Office will accept that a risk might happen in pursuit ofday-to-day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that Post Office are willing and able to tolerate.

Post Office have a five-scale approach to risk appetite, Averse, Cautious, Neutral, Flexible and Open.

There follows a list of applicable Risk Appetite statements for this policy:

Risk Area	Risk Appetite Statement
Ineffective Data Governance **(Information)**	We recommend having an **AVERSE** appetite to risks materialising from unauthorised access to sensitive data, unauthorised changes to data and ineffective processes and procedures for the management of data, (excluding hard copies of data storage)
Ineffective Cyber Security **(Security)**	We recommend having an **AVERSE** appetite to risks materialising from an inadvertent or malicious corruption or modification of data on its IT systems, resulting in service disruption, information modification/destruction
Technical Failures: (Technology)	We recommend a **CAUTIOUS** appetite to risks materialising from software bugs, complete failure of key components, inability to restore data (due to a lack of resilience), failed business change, misaligned contracts and failure to implement new developments correctly (live environment).
Infrastructure Failures: **(Technology)**	We recommend an **AVERSE** appetite to risks materialising from core services failures upon which other services and business functions operate, this includes unsupported Technology Services (software / hardware) and obsolete Technology Infrastructure.

Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required. (See section 1.4 for further details)

2.2. Policy Framework

This policy forms part of the Cyber and Information Security Policy and Standard Set which is located

here: Cyber and Information Security Policy Set (sharepoint.com)

2.3. Who must comply?

Compliance with this Policy is mandatory for all Post Office employees[3] subsidiaries and commercial partners and applies wherever in the world the business is undertaken. All third parties who do business with the Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this Policy with their own equivalent Policy.

Where material non-compliance is identified the matter must be referred to the Policy Owner and Sponsor. Where required, any investigations will be carried out in accordance with the Investigations

[3] In this policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity includ ing employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and contractors.

POL00362894

Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this may be treated as a disciplinary offence.

The next page sets out the minimum control standards that the Post Office has implemented to control these risks.

POL00362894

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks, so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Ineffective Cyber Security	Risks materialising from an inadvertent or malicious corruption or modification of data on its IT systems, resulting in service disruption, information modification/destruction	A Cyber and Information Security Management System (ISMS) must be in place, have senior management approval, be communicated to the entire business and tested for effectiveness. POLs ISMS is comprised of this policy and it's supporting standards, tested by POLs quarterly attestation process.	All Staff	Updated Annually

POL00362894

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Ineffective Cyber Security	Insider Threat Poor controls around the usage of Post Office Information Assets (both digital and physical) by Post Office Staff may impact the Confidentiality, Integrity and Availability of Post Office Data or Impact Post Office reputation by the intentional or accidental misuse of Post Office physical and/or digital assets.	Acceptable Use Standard, Logging and Monitoring Standard, Security Incident Management Standard and Access Control Standard.	All Staff	All the time and evolving with new best practice.
Ineffective Cyber Security	Asset Management Poor understanding of the location, flow and destruction of both physical and digital data assets leads to data loss, corruption, or lack of availability.	Cyber and information Security Standard and Asset Management Standard.	All Staff	All the time and evolving with new best practice.
Technical Failures	Secure Development of business applications Poor design of Business applications or lack of consideration regarding security requirements during the design process can lead to the introduction of security vulnerabilities and subsequently result in breaches of data, loss of integrity or data being accessed by unauthorised individuals.	All projects and programmes must liaise with Cyber Security and the CTO teams for advice and guidance on the security aspects of their designs. All development must comply with the SDLC Standard.	Project & Programme Managers, and procurement.	At project design phase and during change.

POL00362894

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Ineffective Cyber Security	Identity and Access Management Having inappropriate access controls to data owned or processed by Post Office could lead to inappropriate access by unauthorised individuals	All systems must comply with the Access Control Standard.	Data Owners, Line Managers, Project and Programme managers, and procurement.	Whenever a new system is being designed or procured, or when significant change is being applied.
Infrastructure Failures	Security Infrastructure If the design of systems supporting or running security services for Post Office are not securely designed to the industry standards, those functions cannot be assured and Post Office systems and data may be open to attack, causing data breach or loss of confidentiality, integrity and availability.	All projects and programmes must liaise with Cyber Security and the CTO teams for advice and guidance on the security aspects of their designs. All infrastructure must comply with the Platform Security Standard, Cloud Computing Guideline, Network Security Standard, Encryption Standard and the Logging and Monitoring Standard where applicable.	Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time and evolving with new best practice.

POL00362894

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Infrastructure Failures	Network Management If networks supporting the flow of Post Office information are not designed with security in mind, then those networks themselves may contain vulnerabilities causing a loss of confidentiality, integrity or availability of systems and or data.	All network designs must adhere to the Platform Security Standard, Network Security Standard and the Logging and Monitoring Standard where applicable.	Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time and evolving with new best practice.
Ineffective Cyber Security	Mobile and Removeable Devices Poorly controlled mobile and removable devices may lead to a data breach causing a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.	All mobile and removable devices must adhere to the BYOD Standard, Platform Security Standard and the Remote Access and Portable Device Standard where applicable.	All staff	All the time

POL00362894

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Technical Failures	Vulnerability Management If Post Offices devices (laptops, mobiles, network devices, servers etc.) are poorly configured or maintained and those vulnerabilities are exploited then this could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator	All devices must comply with the Vulnerability Standard, Penetration Testing and Vulnerability Scanning Standard, Network Security Standard and the Platform Security Standard.	Cyber Security and CTO, Third party supply chain of IT Services where systems are hosting or processing Post Office data	All the time
Ineffective Cyber Security	Cyber Incident Response Post Office are subject to POL Wide Cyber Incident (e.g. ransomware) which could lead to POL not recovering in a timely manner. If this risk materialised it could result in reputational damage, postmaster dissatisfaction and loss of revenue.	All of Post Office's cyber security protection solutions must adhere to the Security Incident Management Standard and incidents must be assessed, reported and resolved.	Cyber Security and CTO, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time

POL00362894

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Ineffective Data Governance	Data Governance Post Office's data or environment is compromised due to the lack of controls required to manage the creation, usage, destruction or archiving of data and documents used for normal Post Office Operations	All Post Office Data should be managed in line with the Information Classification standard.	All staff	All the time and evolving with new best practice.

POL00362894

3. Where to go for help

3.1. Additional Policies

This Policy is one of a set of policies. The full set of policies can be found on the SharePoint Hub under Policies.

3.2. How to raise a concern

Any Post Office employee who suspects that there is a breach in this Policy should report this without any undue delay, staff may:

- Discuss the matter fully with their Line Manager; or,
- A senior member of the HR Team, or
- Direct to the Whistleblowing Manager (whistleblowing GRO), or
- Contacting the "Speak Up" line, a confidential reporting service which is run by an independent company Convercent:
    - Telephone Number: GRO
    - http://speakup.postoffice.co.uk/ which is a secure on-line web portal

3.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the CISO.

POL00362894

4. Governance

4.1. Governance Responsibilities

The Policy sponsor, takes responsibility at GE level for policies covering their areas.

The Policy Owner is the CISO who is responsible for ensuring that the content is up to date and is capable of being executed. As part of the review process they need to ensure that the minimum controls articulated in the policy are working or to identify any gaps and provide an action plan for remediation.

Additionally, the CISO and the Cyber team are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee as required.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

POL00362894

5. Document Control

5.1. Document Control Record

SUMMARY			
GE Policy Sponsor	Standard Owner	Policy Author	Standard Approver
Zdravko Mladenov	CISO	Head of IT Security	RCC/ARC
Version	Document Review Period	Policy – effective date	Policy location
3.1	Annual	1/3/23	Intranet

REVISION HISTORY			
Version	Date	Changes	Updated by
1.0	12/06/2015	Final QA and release	ISAG
1.1	17/06/2016	Owner details updated to CISO, no further changes after review	ISAG
1.2	20/11/2016	Interim version which was superseded by the new Post Office Operating Model.	ISAG
1.3	26/10/2017	Changed to the new template for policies Changed to reflect the new Post Office structure Minor editorial changes at annual review and a general simplification of the requirements.	IPA & IT Security
1.4	31/10/2017	Updates following Peer review	IPA
1.5	07/12/2018	Minor updates on annual review – caused by changes in responsibilities	IPA
2.0	14/01/2020	Updated policy to also include statement to merge Acceptable Use, IT Security and Document Retention and Disposal. Approval from RCC	IT Security
2.0	29/07/2021	Updated Whistleblowing details	Reena Chohan
3.0	14/12/2021	Minor updates on annual review	Tony Jowett
3.1	6/01/2023	Minor update to reflect changes in document names and formatting.	Cyber Security

5.2. Oversight Committee: Risk and Compliance Committee / Audit and Risk Committee

Committee	**Date Approved**
POL R&CC	14/03/23
POL ARC	28/03/23
POMS ARC	TBC
PZBPL Board	TBC

Next Policy Annual Review Date: March 2024

POL00362894

5.3. Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Payzone Bill Payment Limited is a limited company registered in England and Wales under company number: 11310918. VAT registration number GB 172 6705 02. Registered office: Finsbury Dials, 20 Finsbury Street, London, England EC2Y 9A