IT Security Standard

Logging and Monitoring

Version – V2.2

POL00362912

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 Logging and Monitoring Standard is to provide baseline security requirements for logging and monitoring of user and system activities. These activities are critical in detecting, preventing, and minimising the impact of a data compromise. This standard will:

- Identify the scope of systems and equipment to which the standard applies.
- Define key processes that support the implementation of this standard.

1.3 Core Principles

Compliance with this standard will aid in ensuring that logging and monitoring will be conducted in accordance with Information Security requirements and industry best practice. By following this Standard the following principles should be met:

- By managing log files in a consistent way Post Office will be able to investigate and recover from security events more efficiently
- Post Office will be able to meet their legal and regulatory obligations
- Log files are only kept for as long as necessary
- The confidentiality, integrity and authenticity of log files are maintained

1.4 Application

The Logging and Monitoring Standard applies to all Post Office staff responsible for Post Office Systems, including third party suppliers providing services to, for, or on behalf of Post Office, and aligns to the requirements of the IT Security Policy.

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.

POL00362912

3 Regulation

Monitoring of communications, in respect to rights of privacy and private correspondence, shall be undertaken in accordance with the UK Regulation of Investigatory Powers Act 2000 (RIPA), Human Rights Act 2000 (HRA) and the Data Protection Act 2018

4 Log Collection

Where contractually agreed with the Post Office, all IT devices that store or process Post Office's information must be monitored for user auditing and security events.

Monitored components will include, but not be limited to, applications, operating systems, databases, middleware, storage, network, security equipment and software relating to or supporting Post Office environment.

Users must be prevented from tampering with the reporting of events from the monitored device.

Automated audit trails for all system components must be capable of reconstructing the following events as a minimum:

- User authentications, both successful and failed attempts.
- All individual access to cardholder data, including successful events.
- All actions taken by any individual with root or administrative privileges.
- Access to all audit trails.
- Password changes
- Scans on your firewall's open and closed ports. Malware detection
- Malware attacks seen by IDS /IPS
- Denial of service attacks
- Errors on network devices
- File name changes
- File integrity changes
- Data exported
- New processes started or running processes stopped
- Shared access events
- Disconnected events
- New service installation
- File auditing
- New user accounts
- Modified registry values
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- .
- Creation and deletion of system-level objects.
- Changes to access or user privileges.
- Changes to configuration on dedicated security devices.
- Changes to security configuration.
- Initialisation, stopping, or pausing of the audit logs

Record at least the following entries for each event:

- User ID.
- Date and time.
- Success or failure indication.
- Origination of event.
- Event type.
- Identity or name of affected data, system component or resource

Supplier must agree to forward security logs from Post Office's utilised infrastructure to the Post Office logging and event management (SIEM) solution in a secure manner at their own cost.

4.1 Log Management and Protection

Secure audit trails so they cannot be altered. This includes the following:

- Limit viewing of audit trails to those with a job related need.
- Protect audit trail files from unauthorised modifications.
- Promptly back up audit trail files to a centralised log server or media that is difficult to alter.
- Ensure that existing log data cannot be modified without generating alerts.

All system clocks must be accurate, protected and synchronised with industry-accepted time sources (please see the Platform Security Standard)

Failure of any individual component of the log collection solution or supporting network infrastructure must not result in the loss of, or failure to, collect log data.

4.2 Log Analysis

Security logs must be accessible when required to allow analysis in a timely manner.

Where log capture, storage and analysis is in place, security logs and events for all system components (including critical servers, firewalls, IDS/IPS, authentication server, e-commerce, system that store, process or transmit cardholder data etc.) must be reviewed at least daily (if not in real-time) to ensure that security incidents are identified efficiently.

Review logs from other system components periodically based on the POL risk management strategy.

Segregation of duties must occur to ensure no conflict of interests exist between monitoring duties and administration.

Logs must only be accessible by authorised individuals on a 'need-to-know' basis, as per the Access Control Standard.

4.3 Log Storage and backup

All security logging of physical infrastructure must be held in a secure central repository.

The Supplier shall make logs available on demand if a security investigation requires evidence.

Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis or longer if stipulated by specific regulatory requirements.

The Supplier will maintain chain of custody of event logs so that the data can be presented as evidence in court, if required.

Logs must be removed in a secure manner on expiry of the retention period.

Logs must be backed up at least daily.

Critical Post Office logs must be backed up to a different location to where the original data is stored.

If the log file being backed up is encrypted, th e back-up must also have an equivalent level of encryption applied.

Log recovery testing must be performed on a regular basis.

4.4 Audit Logging

The Cyber Security Operation /Supplier shall be accountable for ensuring that the security monitoring process is defined and operating.

The scope of monitoring must be defined, maintained in an inventory and reviewed with Cyber Security at least annually.

5 Minimum controls

The table below sets out the minimum control standards.

Control Ref	Control Objective	Control Guidelines
PHT0291	Establish, implement, and maintain Security Control System monitoring and reporting procedures.	Include detecting and reporting the failure of a change detection mechanism in the Security Control System monitoring and reporting procedures. Include detecting and reporting the failure of audit logging in the Security Control System monitoring and reporting procedures. Include detecting and reporting the failure of an anti-malware solution in the Security Control System monitoring and reporting procedures Include detecting and reporting the failure of a segmentation control in the Security Control System monitoring and reporting procedures. Include detecting and reporting the failure of a physical access control in the Security Control System monitoring and reporting procedures. Include detecting and reporting the failure of a logical access control in the Security Control System monitoring and reporting procedures. Include detecting and reporting the failure of an Intrusion Detection and Prevention System in the Security Control System monitoring and reporting procedures. Include detecting and reporting the failure of a firewall in the Security Control System monitoring and reporting procedures.
PHT0300	Establish, implement, and maintain Responding to	Include resuming security system monitoring and logging operations in the Responding to Failures in Security Controls procedure.

Control Ref	Control Objective	Control Guidelines
	Failures in Security Controls procedures.	Include implementing mitigating controls to prevent the root cause of the failure of a security control in the Responding to Failures in Security Controls procedure. Include performing a risk assessment to determine whether further actions are required because of the failure of a security control in the Responding to Failures in Security Controls procedure. Include correcting security issues caused by the failure of a security control in the Responding to Failures in Security Controls procedure. Include documenting the duration of the failure of a security control in the Responding to Failures in Security Controls procedure. Include restoring security functions in the Responding to Failures in Security Controls procedure.
PHT0307 CTRL0020655	Establish, implement, and maintain logging and monitoring operations.	Enable monitoring and logging operations on all assets that meet the organizational criteria to maintain event logs. Establish, implement, and maintain intrusion management operations.
PHT0310	Install and maintain an Intrusion Detection System and/or Intrusion Prevention System.	Protect each person's right to privacy and civil liberties during intrusion management operations. Monitor systems for inappropriate usage and other security violations.
PHT0313	Monitor systems for access to restricted data or restricted information.	Assign roles and responsibilities for overseeing access to restricted data or restricted information. Alert interested personnel when suspicious activity is detected by an Intrusion Detection System or Intrusion Prevention System.
PHT0316 CTRL0020718	Monitor systems for unauthorized mobile code.	Unauthorized mobile code is detected. Control and monitor the use of mobile code
PHT0317	Update the intrusion detection capabilities and the incident response capabilities regularly.	The organization must keep the signatures on signature-based Intrusion Detection Systems up-to-date.
PHT0318	Define and assign log management roles and responsibilities.	The organization should assign responsibility for monitoring on a regular basis

Control Ref	Control Objective	Control Guidelines
		As part of the log management planning process, an organization should define the roles and responsibilities of individuals and teams who are expected to be involved in log management.
PHT0319	Operationalize key monitoring and logging concepts to ensure the audit trails capture sufficient information.	Establish, implement, and maintain event logging procedures. Include a standard to collect and interpret event logs in the event logging procedures. Compile the event logs of multiple components into a system-wide time-correlated audit trail. Review and update event logs and audit logs, as necessary.
PHT0324	Correlate log entries to security controls to verify the security control's effectiveness.	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measure
PHT0325	Identify cybersecurity events in event logs and audit logs.	Follow up exceptions and anomalies identified when reviewing logs.
PHT0327	Document the event information to be logged in the event information log specification.	The organization should identify indicators to be monitored. The indicators should be linked to thresholds to enable the organization to act on the risks quickly
PHT0328	Enable logging for all systems that meet a traceability criteria.	The audit trail must provide for individual accountability to ensure all actions taken by a user are associated with the user where applicable
PHT0329	Synchronize system clocks to an accurate and universal time source on all devices.	A trusted time source should be used to time-stamp the database event logs.
PHT0330	Review and update the list of auditable events in the event logging procedures.	Establish, document, and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment
PHT0331 CTRL0020527	Monitor and evaluate system performance.	Critical services are monitored through event logs. Exceptions raised through monitoring alert the appropriate staff members and are logged, escalated and remediated.

Control Ref	Control Objective	Control Guidelines
		Event logs are retained for an appropriate period of time.
PHT0332 CTRL0020713	Monitor for and react to when suspicious activities are detected	The organisation must configure systems and network devices to log suspicious or anonymous behaviour, such as invalid logon attempts, out of hours failed access attempts, network penetration attempts and other security activity. Logs from different sources are adequately secure, aggregated and analysed by a SIEM tool and identified security violations escalated to senior management in a timely manner
PHT0336	Implement file integrity monitoring.	Changes which could affect the security of the service should be identified and managed. Unauthorised changes should be detected
PHT0337	Monitor and evaluate user account activity.	The use of privileged accounts, and any activities undertaken with them, are monitored and audited. Break glass accounts are monitored and audited for unauthorised use or modification At least once a month, the activations of the emergency users and the corresponding approvals are compared manually. Irregularities are examined in order to determine any misuse of these users and to avoid this in the future.
PHT0338	Establish, implement, and maintain a risk monitoring program.	Monitor the organization's exposure to threats, as necessary. Monitor for new vulnerabilities.

6 Where to go for help

6.1 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/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 Service Desk.

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 Cyber Security Team via cyber GRO

7 Version Control

7.1 Version Control

Date	Version	Updated by	Change Details
04/05/18	0.1	IT Security	Changed to the new template for standards Changed to reflect the new Post Office structure First Draft
22/05/18	0.2	IT Security	Updated post peer review
01/06/18	1.0	IT Security	Final Approved version
04/11/2021	2.0	IT Security	Updated the standard according to the PCI DSS security requirements.
04/04/2023	2.1	Cyber Compliance	Updated to align with control framework
25/04/2023	2.2	Cyber Compliance	CSF Approval for publication

7.2 Standard Approval

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