[Company]

LOGGING AND MONITORING POLICY

System monitoring and logging

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Logging and Monitoring Policy

3.1 Purpose

The purpose of this policy is to address the identification and management of risk the of system-based security events by logging and monitoring systems.

To record events and gather evidence.

3.2 Scope

All company employees and external party users.

All devices used to process, store, or transmit company information.

3.3 Principle

All devices that process, store, or transmit confidential, card holder or personal information have audit and logging enabled, where logging is possible and practical and can generate audit logs.

3.4 Event Logging

Event logs recording user activities, exceptions, faults, and information security events should be produced, kept, and regularly reviewed.

Event logs should include, when relevant:

- user IDs.
- system activities.
- dates, times, and details of key events, e.g., log-on and log-off.
- device identity or location if possible and system identifier.
- records of successful and rejected system access attempts.
- records of successful and rejected data and other resource access attempts.
- changes to system configuration.
- use of privileges.
- use of system utilities and applications.
- files accessed and the kind of access.
- network addresses and protocols.
- alarms raised by the access control system.
- activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.
- records of transactions executed by users in applications.
- identity or name of affected data, system component, or resource.

Automated monitoring systems which can generate consolidated reports and alerts on system security are used where possible.

3.5 Event Logging Access Control

Event logging and monitoring is performed by authorised personnel only.

Event logging and monitoring systems and reports are strictly protected and restricted in line with the access control policy and data retention schedule.

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities.

3.6 Protection of Event Log Information

Logging facilities and log information should be protected against tampering and unauthorized access.

Controls protect against unauthorized changes to log information and operational problems with the logging facility including:

- alterations to the message types that are recorded
- log files being edited or deleted
- storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

3.7 Administrator and operator logs

System administrator and system operator activities should be logged, and the logs protected and regularly reviewed.

Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.

An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

3.8 Clock synchronisation

The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.

Time data is protected.

Time settings are received from industry-accepted time sources.

3.9 Event Log Monitoring

Responsibilities are assigned for the analysing and monitoring of events.

High risk events automatically alert to the incident management process.

Log files are reviewed daily.

The following shall be reviewed daily:

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD
- Logs of all critical system components
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

3.10 Event Log Retention

Event logs from the last 3 months are immediately available.

Event logs are retained for 12 months.

3.11 Centralised Logging

Centralised logging to a remote dedicated log server should be considered.

3.12 Personal Privacy

Privacy of employees and customers is respected in line with legal and regulatory requirement, including but not limited to GDPR and the Data Protection Act 2018

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.