Document Reference Number	**UoG/ILS/IS 018**
Title	Policy for Logging and Monitoring
Owning Department	Information and Library Services
Version	1.2
Approved Date	10/12/2024
Approving Body	IT Management Board (IM)
Review Date	09/12/2025
Classification	Public – non-sensitive

Version Control

Version	**Last Modified**	**Last Modified By**	**Document Changes**
1.2	10/12/2024	Atif Siddique	Added version control.

Policy for Logging and Monitoring

1.0 Purpose

1.1 To address the identification and management of risk of system-based security events through monitoring and logging.

1.2 To record events and gather evidence.

2.0 ISO 27001 Reference

2.1 This policy complies with the university's information security strategy and draws upon the ISO 27002 Code of Practice.

3.0 Scope

3.1 This policy applies to all staff, students, contractors and third-party agents who access, use, process or manage the university's information assets.

3.3 All devices used to process, store, or transmit university information.

4.0 Logging and Monitoring

4.1 All devices that process, store or transmit information should have auditing and logging enabled where possible.

4.2 **Event Logging**

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

Where relevant, event logs should include, but not be limited to the following:

- user IDs
- system activities
- dates, times and details of key events eg log-on and log-off
- device identity or location and system identifier
- records of successful and unsuccessful system access attempts
- records of successful and unsuccessful data and other resource access attempts
- changes to system configuration
- use of privilege
- use of system utilities and applications
- file access including access type
- network addresses and protocols
- alarms raised by the access control system
- activation and deactivation of protection systems such as anti-virus and intrusion detection systems

- records of transactions executed by users in applications

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

4.3 Event Logging Access Control

Event logging and monitoring must be performed by authorised individuals, using authorised tools only.

4.3.1 Logging and monitoring systems and reports are strictly restricted to those individuals who are required to manage these systems as required by their role. The necessary measures must be implemented to ensure unauthorized access to these systems prevented.

4.4 Protection of Event Log Information

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

4.4.1 Relevant controls should be implemented to protect against unauthorised changes to log information and operational issues with the logging facilities including:

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

4.5 Administrator and Operator Logs

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

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

4.5.2 A system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

4.6 Clock Synchronisation

The clocks of all relevant information processing systems should be synchronized to a single reference time source.

4.6.1 Time data should be protected.

4.6.2 Time settings should be received from university approved time sources.

4.7 Event Log Monitoring

Responsibilities for the analysis and monitoring of events must be assigned.

4.7.1 Critical alerts and events considered as high risk should automatically alert to the cyber security team and where necessary the university's cyber incident response plan should be initiated.

4.8 Event Log Retention

4.8.1 General purpose logs should be held for a minimum of 30 days.

4.8.2 On campus user internet access logs should be held for three months, as per JISC recommendation.

4.9 Centralised Logging

Where relevant, centralised logging to a remote dedicated logging service should be implemented.

4.10 Personal Privacy

Privacy of staff, students and other stakeholders shall be respected in line with the university's legal and regulatory requirements.

5.0 Policy Compliance

5.1 The necessary steps to verify compliance with this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

5.2 Failure to adhere to this policy may be addressed under the university's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the Information security policies.

6.0 Exception to Policy

Any exception to this policy must be approved by the Executive Director and Chief Information Officer or a nominee.

7.0 Policy Review and Maintenance

This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

8.0 Related Policies, Procedures and Standards

- Information security policies and associated documents
- Information compliance policies and associated documents