THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Standard

Monitoring and Logging for Malicious Events

Introduction

Monitoring and logging of LSE systems for malicious events is carried out to prevent attacks upon LSE identities, systems, services and data, and to assist with retrospective forensic investigations.

Monitoring and logging at LSE is conducted with regard to the privacy of users, the requirements of UK GDPR, the Data Protection Act (2018) around Personal Data, and the principles of 'least privilege' and 'need to know' for data use as embedded in the Cyber Security Policy.

This standard enables us to meet requirements laid out in the Conditions of Use of IT Facilities at LSE. It is critical to implementing and maintaining the Cyber Security Policy's approach to maintaining the Confidentiality, Integrity and Availability of LSE's systems and data.

Purpose

This standard sets out LSE's monitoring and logging requirements for the effective detection and remediation of malicious events. It does so in a technology agnostic way. The intention of the standard is to ensure we can:

1. Alert on and contain malicious events as quickly as possible
2. Inform appropriate remediation activities to prevent incident recurrence.
3. Minimise the opportunity for identity, application, system and service compromise, contain data loss.
4. Prevent, where possible, malicious activities being carried out on or by using LSE's IT resources.
5. Provide consistent evidence to support investigations into malware outbreaks, environment compromise and other malicious use of or intrusions into LSE facilities.

Standard/Requirements

1. LSE will respond to alerts with a *risk-averse* approach i.e. prioritising a swift response and the minimisation of the risk of damage to LSE assets.
2. LSE will monitor and log appropriately to
    a. maintain the security of its IT environments, as defined in the scope.
    b. Detect potentially malicious events, quarantine assets involved (if owned or operated by LSE) or block them from our systems and network (if not owned or operated by LSE)
    c. Reconstruct the path of malicious activities after the event, or enable a third party to do so on our behalf (i.e. a forensics form)

3. LSE will use commercial threat detection systems and, where necessary, additional contracted security operations to enable appropriate detection, threat hunting and responsive operations.
4. Monitoring consoles and logs will only be accessible to appropriate staff, and will have available information restricted according to role, under the 'least privilege' and 'need to know' approach embedded in the Cyber Security Policy.
5. Logs by default are retained for 90 days, following recommendations put forward by Jisc unless there are legal or practical reasons for other limits (e.g. storage limits necessitating faster rollover of data).
6. Where the responsibility for detecting and remediating malicious events is incumbent upon a third party (e.g. because it is a SaaS platform, or because they are the Data Processor), their capabilities for achieving equivalence with this standard will be assessed by LSE either through assessment of how they meet our functional and non-functional requirements, or through a Cloud Assurance Questionnaire, the responses to which must be judged as satisfactory before the service is commissioned.

Scope

This standard applies to LSE IT networks, Infrastructure as a Service (e.g. LSE-operated instances in AWS, Azure and other IaaS environments), productivity platforms, servers, applications, storage, identities and endpoints.

Responsibilities

Chief Information Officer – is accountable for DTS's monitoring and logging services.

Director of Cyber Security – is responsible for maintaining an overall cyber security monitoring and response service, including LSE's use of a Managed Security Operations Centre and a Managed Security Incident and Event Monitoring service. Responsible for the risk averse response approach.

Head of Information Security – is responsible for running the day-to-day monitoring and cyber incident response operations.

Head of Platforms – is responsible for the management of security consoles, allocating appropriate access, implementing XDR/EDR clients on centrally-managed servers, and for monitoring and alerting on centrally managed servers, productivity platforms, containers and IaaS instances.

Head of Networks – is responsible for monitoring and alerting on network security, including the blocking of endpoints from accessing the LSE network, and preventing campus-wide access to malicious URLs or IP addresses.

Service Lines Manager, End User Computing – is responsible for implementing XDR/EDR clients on centrally-managed endpoints, and for the monitoring and alerting on end user devices, including endpoint isolation and quarantine where required.

Business Led Technology Teams and other non-DTS service and server administrators – are responsible for ensuring suitable XDR/EDR is installed on servers, that suitable logs are

maintained and appropriate monitoring for breaches is undertaken in their areas, responding to alerts they receive, and escalating where necessary to the Information Security Team.

Director of Strategy and Architecture – is responsible for ensuring commissioned solutions meet this standard.

Supporting/Relevant documents

- *Cyber Security Policy*
- *Conditions of Use of IT Facilities at LSE*

Document Control

Standard owner:	Director of Cyber Security
Standard author:	Jethro Perkins
Responsible office:	DTS
Approving body:	Policy Working Group
Effective date:	01 July 2026
Date of next review:	01 July 2029
Review schedule:	3 years

Version history

Whole numbers should represent significant revisions of the policy, decimals should be used to indicate minor amendments. E.g. version 2 would represent a wholescale review and update, whereas 2.1 would represent minor technical updates that do not change the nature or implementation of the policy.

Version	Date	Approved by	Details of amendments
V0.1	11 December 2025	Policy Working Group	Initial version, adapted from the Monitoring and Logging Policy
V1.0	05 June 2026		Adapted to fit the standard template. Minor amendments for clarity.
V1.1	24 June 2026	Policy Working Group	Minor grammatical updates