London School of Economics & Political Science

IT Services

Policy

Monitoring and Logging Policy

Jethro Perkins

Information Security Manager

Summary	This policy outlines the monitoring and logging processes that takes place of IT facilities at LSE.
Version	Draft 2.2
Date	18 May 2018
Library reference	ISM-PY-105

1 Introduction

The information held within and managed by the London School of Economics (LSE) shall, where possible, be protected against the consequences of breaches of confidentiality, failures of integrity or interruptions of its availability to authorised users. For an effective approach to information security, the participation and support are required of all LSE staff, students and other authorised users.

Monitoring and logging of LSE systems will be carried out in order to help protect the safety of the LSE user community, to prevent attacks upon LSE systems, and in order to preserve the confidentiality, integrity and availability of the data held upon LSE information systems. It will also assist LSE in capacity planning by analysing usage patterns and warning before systems and services reach capacity. Monitoring and logging at LSE is carried out with regard to the privacy of users, the requirements of the General Data Protection Regulation (GDPR) around Personally Identifiable Information, and the principles of ‘least privilege’ and ‘need to know’ for data use as embedded in the Information Security Policy.

Failure of LSE to appropriately log and monitor defined activities could lead to breaches in confidentiality, integrity and availability of data and systems through the following conditions:

1. LSE fined up to €20million or 4% of turnover for a breach of confidential data under the GDPR
2. Systems and servers confiscated and/or destroyed by the police due to the presence of illegal content
3. Prosecution of LSE data owners due to the presence of illegal content
4. LSE fined up to £250,000 for hosting illegally copied material
5. LSE blacklisted by Internet Service Providers due to spam sent from compromised accounts.
    a. Accounts compromised by entering data into phishing websites.
    b. Phishing websites available due to lack of web content filtering.
6. LSE blocked from using segments of the internet due to spam sent from compromised LSE accounts
7. Integrity of data unverifiable after access by compromised accounts
8. Confidentiality, Integrity and Availability of data destroyed by unmonitored malicious and/or mobile code activity
9. LSE system and network performance degradation due to the operation of unmonitored and/or unapproved applications, affecting availability of legitimate and business critical applications
10. LSE system and network performance degradation due to inadequate capacity planning

Information security at LSE is governed by its *Information Security Policy*, a number of subsidiary policies and applicable laws, such as the General Data Protection Regulation, the Regulation of Investigatory Powers Act 2000, the Computer Misuse Act 1990 and the Statutory Guidance to the Counter Terrorism and Security Act 2015. This subsidiary policy covers the monitoring and logging of uses of information technology within LSE. It is the responsibility of every user of LSE’s IT systems to know these policies, and to conduct their activities accordingly.

1.1 Scope

This policy applies to all LSE networks, IT systems, devices on the LSE network, devices owned by LSE (whether on or off the LSE network), Cloud services used by LSE, authorised users *and* unauthorised users.

2 Policy

2.1 Principles

LSE's networks, computers, and any provided service, system and application provide a level of automated logging and monitoring. This logging and monitoring may be carried out by IMT, a business-led IT function, by a service provider on our behalf (such as a Cloud service provider, or our Internet Service Provider), or by any mixture of the above. Logging and monitoring are used for the following purposes:

1. Tracking the flow of network traffic and ensuring the availability of network bandwidth
2. Facilitating and improving capacity planning
3. Identifying areas for improvement, including provision of teaching, learning and research facilities
4. Ensuring use of resources is authorised and detecting unauthorised access
5. Management of systems and services
6. Ensuring system and service security
7. Compliance with LSE policies, legal and contractual requirements and any other appropriate regulations all LSE users must comply with (e.g. the Joint Academic Network [JANET] Acceptable Use Policy)
8. Avoiding or mitigating legal liabilities and complying with legal obligations
9. Preventing and detecting crime
10. Limiting the damage from malware and phishing attacks, and preventing their further spread

2.2 Monitoring performed by members of IMT

Staff from particular IMT teams routinely perform monitoring of:

- bandwidth usage,
- network availability,
- system availability and performance
- service/application availability and performance
- patching level of Operating Systems, software and applications
- software installations including licensing

This monitoring is only carried out by authorised staff. Access to monitoring tools and data is controlled using 'need to know' and 'least privilege' principles.

Monitoring will include periodic simulated attacks by users authorised by the Information Security Team to test or verify the security of systems.

IMT does not perform *any* routine monitoring of:

- use of services by individuals
- device use
- Internet use by individuals
- email use

2.3 Other monitoring

Business-led IT functions are responsible for monitoring the systems and services they manage and maintain. Monitoring must be performed by designated staff members or teams, with access following 'need to know' and 'least privilege' principles.

2.4 Exceptional monitoring

If required by law, or by a law enforcement official with the appropriate authorisation, or as directed by a 'request for access' form signed and authorised by a member of the Senior Management Committee, IMT or any business-led IT function will as appropriate undertake exceptional monitoring functions as required.

2.5 Automated filtering

2.5.1 Anti-malware

Filtering by automated systems, including actions where relevant (such as blocking access, or performing automatic cleanup) is performed in the detection, blocking or removal of viruses, malware, spam, pornography, and illegal content (e.g. illegally downloaded copyright-controlled content).

Internet traffic from LSE is automatically monitored by our Internet Service Provider (Jisc) for malware.

2.5.2 Data Loss Prevention

Automated filtering is used in LSE's Office365 tenancy (OneDrive, SharePoint, Exchange) to detect and prevent the insecure transfer of personal data outside LSE's systems.

The content of files is not scanned.

A log of filtering activities will be kept for two years, in order to understand the yearly patterns of activities.

File use is not monitored by IMT staff.

2.5.3 Email filtering

Incoming e-mail will be automatically scanned by our email provider's filtering system. This includes algorithms used to detect and block the transmission of sensitive data, malware, spam, phishing, spoofed and junk email.

The content of email messages is not scanned.

A trace log of emails sent by and to user accounts will be kept on a 30-day rolling basis.

Email use is not monitored by IMT staff.

2.5.4 Web content filtering

Web content filtering is governed by the Web Content Filtering Policy: (https://info.lse.ac.uk/staff/divisions/imt/services/infosec/resouces/web-content-filtering).

No logs are kept of web content filtering actions.

2.6 Logging

The following activities are logged by default:

- Workstation logon/logoff (username)
- Server logon/logoff (username)
- Application access (by username, IP address)
- Anti-virus events (username, workstation)
- Firewall traffic (source IP, destination IP)
- DHCP leases form both wired and wireless traffic (MAC address)
- Wireless IP location (MAC address, IP address)

Logs by default are kept for 90 days, following recommendations put forward by Jisc (see https://community.jisc.ac.uk/library/janet-services-documentation/using-logfiles), unless:

- there are legitimate business reasons for logs to be held for a longer period of time (e.g. Moodle, where logs provide proof of student engagement, ResourceLink where logs provide proof of user access to sensitive personal information, LSE for You where application logs record access to sensitive personal data)[i]

- There are legal, regulatory or contractual reasons to hold logs for longer (e.g. employment law, financial regulations)
- Log space is configured to roll over after size limits are reached (workstations)
- the application's log retention does not permit configuration (Sophos anti-virus, where infection events are indefinitely retained)
- We are using cloud services where log retention configuration is not within our control
- There is no Personally Identifiable Information, in which case logs are stored indefinitely

Logs are kept appropriately secure from unauthorised access and tampering. They are made available to the team responsible for maintaining the service, and the Information Security Team upon request, in the event an investigation is required.

2.7 Logging by other Divisions and Departments

Logging by other Divisions and Departments will meet the standards outlined in 2.6 above.

2.8 Unauthorised Use

Unauthorised use, as outlined in the *Information Security Policy* and associated policies, may give rise to disciplinary procedures and/or criminal prosecution.

Evidence of unauthorised use collected during logging and monitoring may be used subsequently in disciplinary, criminal or other proceedings.

2.9 Laws and regulations affecting LSE monitoring and logging

2.9.1 Regulation of Investigatory Powers Act 2000

The legislation requires LSE to intercept communications without consent, where directed by law enforcement officials, for purposes such as recording evidence of transactions, detecting crime or unauthorised use. LSE is not required to gain consent before intercepting for these purposes, but needs to inform staff and students that interception may take place. This does not imply that all communications are monitored, just that they may be for the above purposes. The Act is available here: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

2.9.2 General Data Protection Regulation

IMT hold user registration data and information on the use of the LSE's computer systems and network in accordance with the stipulations of the General Data Protection Regulation, to ensure personally-identifiable information ion log data is not made accessible outside of the specified groups responsible for maintaining services. Information concerning when and where users have accessed systems, print logs, Internet caches, access control system data, network traffic statistics and other similar data may be logged, but access will be strictly controlled and logs will be held for no longer than necessary.

While normally only used for resolving operational problems, these logs will be analysed in a controlled environment (under the remit of the LSE's Information Security Policies) in the case where a breach of LSE regulations and policies, or other misuses and abuses of facilities, is suspected or identified.

Information contained within the logs referred to above may also be used to communicate with users to alert them to malfunctions within LSE IT facilities or to request action to correct the malfunctions which may be putting normal operations of the IT facilities in jeopardy.

[i] This is also recommended by Jisc within the same document: "users of university and college computers will usually be students or staff. Both of these legal relationships involve much longer retention periods to comply with education and employment law, so information about these users' identities will normally and legitimately be held for much longer than six months."

If log information is held outside LSE, it will still be held under the auspices of the General Data Protection Regulation, with access accordingly controlled.

Further information about the General Data Protection Regulation is available here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

2.9.3 Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.

In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances. The Terrorism Act is available here:

http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_2

2.9.4 Jisc Joint Academic Network Acceptable Use Policy

LSE's internet service provider, Jisc requires that LSE is able to identify any person using the Janet service.

The Janet Acceptable Use Policy can be found here: https://community.ja.net/library/acceptable-use-policy

2.9.5 Counter-Terrorism and Security Act 2015 – Statutory Guidance

The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 (Prevent duty guidance for higher education institutions in England and Wales https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf) requires LSE to have "due regard to the need to prevent people from being drawn into terrorism."

The Act imposes certain duties under the *Prevent* programme, which is aimed at responding to "the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views." The Prevent programme also aims to provide "practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support".

LSE must balance its existing legal commitments to uphold academic freedom and (under the Education (No. 2) Act 1986) freedom of speech within the law against the new Prevent duty, and seek to ensure that its IT facilities are not used to draw people into terrorism.

2.10 ISO27001 controls governing LSE use of monitoring

The necessity of monitoring and logging is covered by the International Standards Organisation's information security standard ISO27001, in the following control sets:

A.8.2.3: Handling of Assets

A.9.4.1: Information Access Restriction

A.12.1.3: Capacity Management

A.12.2.1: Controls against malware

A.12.4.1: Event logging

A.12.4.2: Protection of log information

A.12.4.3: Administrator and operator logs

2.11 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE's overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website.

2.12 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IMT as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

3 Responsibilities

IMT
Monitoring and log analysis of network activity and centrally-managed LSE IT systems will only be undertaken by members of IMT, as appropriate to their area, or by third parties explicitly appointed by IMT for this purpose, who will act under Non-Disclosure Agreements (NDAs).

Centrally-managed logs are kept secure and will only be accessed by authorised members of IMT as outlined above.

Business-led IT functions
Monitoring and Logging of non-IMT systems the responsibility of system owners.

Logs must be kept secure and will only be accessed by authorised members of staff.

Business owners of Cloud services
Logging requirements of the business function and providers' logging capabilities must be established by the owner of a business function before commissioning Cloud services. The Cloud Assurance Questionnaire explicitly addresses logging.

LSE Estates
Monitoring and logging of Building Management Systems, including CCTV and door controllers.

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3.18	07/02/18	Jethro Perkins
Information Classification Standard	3.0	15/03/13	Jethro Perkins
JANET Acceptable Use Policy	12	May 2016	
Prevent Duty Guidance for Higher Education Institutions in England and Wales	(no version)	18/09/15	Home Office

Version history

Date	Version	Comments
16/04/13	0.1	Initial version
23/04/13	1.0	Updated links, included more information on ISO27001 controls. Submitted to ISAB
07/05/13	1.1	Updated in light of ISAB comments
18/06/13	1.2	Updated Sections 1 and 3.5. in order to reflect comments by ITC members
04/01/16	1.3	Updated Sections 1 and 3 to explicitly mentions LSE's statutory Prevent duties as mandated by the Counter Terrorism and Security Act 2015. Removal of 'Library' from Responsibilities section, as internal library IT systems are now managed by IMT
07/02/18	2.0	Rewrite, taking into account Cloud services and user concerns about active monitoring.

Review control

Reviewer	Section	Comments	Actions agreed
ITC	1	Emphasise the benefits of monitoring and logging e.g. safety and security and in identifying capacity issues	Section updated
ITC	3.5	Clarify the description of the legal stipulations around monitoring and logging	Section updated