

Policy

Monitoring and Logging Policy

Jethro Perkins

Information Security Manager

Summary	This document outlines the controls from ISO27002 that relate to the LSE's Information Security Policy and Infrastructure that apply to the LSE, across all departments.
Version	Release 1.3
Date	04 January 2016
Library reference	ISM-PY-105

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3.0	12/03/13	Jethro Perkins
Information Classification Standard	2.1	12/03/13	Jethro Perkins
JANET Acceptable Use Policy	11	May 2011	
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

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

Table of contents

1	Introduction	4
1.1	Scope	4
2	Responsibilities.....	5
3	Monitoring.....	6
3.1	Principles.....	6
3.2	Email scanning.....	6
3.3	Consent.....	6
3.4	Unauthorised Use.....	6
3.5	Laws and regulations affecting LSE monitoring and logging	7
3.5.1	<i>Regulation of Investigatory Powers Act 2000.....</i>	7
3.5.2	<i>Data Protection Act 1998.....</i>	7
3.5.3	<i>Terrorism Act 2006</i>	7
3.5.4	<i>Janet Acceptable Use Policy</i>	7
3.5.5	<i>Counter-Terrorism and Security Act 2015 – Statutory Guidance.....</i>	8
3.6	ISO27001 controls governing LSE use of monitoring	8
3.7	Further Policies, Codes of Practice, Procedures and Guidelines	8
3.8	Review and Development	9

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 to 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 of its information technology systems.

Monitoring and logging of LSE systems will be carried out in order to help protect the safety of the LSE user community, 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 for the areas of teaching facilities and learning materials by analysing usage patterns and warning before systems reach capacity.

Failure of LSE to monitor content could lead to failures in confidentiality, integrity and availability of LSE data and systems through the following conditions:

1. Systems and servers confiscated and/or destroyed by the police due to the presence of illegal content
2. Prosecution of LSE data owners due to the presence of illegal content
3. LSE fined up to £250,000 for hosting illegally copied material
4. LSE blacklisted by Internet Service Providers due to spam sent from compromised accounts. Accounts compromised by entering data into phishing websites. Phishing websites available due to lack of content filtering.
5. LSE blocked from using segments of the internet due to spam sent from compromised LSE accounts
6. Integrity of data unverifiable after access by compromised accounts
7. Confidentiality, Integrity and Availability of data destroyed by unmonitored malicious and/or mobile code activity
8. LSE system and network performance degradation due to the operation of unmonitored and/or unapproved applications, affecting availability of legitimate and business critical applications
9. 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 Data Protection Act 1998, 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 all 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, authorised users *and* unauthorised users.

2 Responsibilities

IMT

Monitoring and log analysis of LSE IT systems will only be undertaken by members of the Systems, Networks or Information Security teams within Information Management and Technology, or by third parties explicitly appointed by IMT for this purpose, who will act under Non-Disclosure Agreements (NDAs).

Logs are kept secure and will only be accessed by authorised members of IMT as outlined above.

Logs will only be kept as long as necessary, in line with current data protection guidelines.

STICERD

Monitoring and Logging of STICERD systems will be undertaken by STICERD IT staff.

Logs are kept secure and will only be accessed by authorised members of STICERD IT staff.

Logs will only be kept as long as necessary, in line with current data protection guidelines.

3 Monitoring

3.1 Principles

Networks, computers, internet usage and email usage may be monitored by members of the Networks, Systems and Information Security teams within IMT, or third parties contracted on behalf of IMT, and usage logged. Logs are kept secure and are only available to networks, Systems and Information Security teams, and will only be kept as long as necessary, in line with current data protection guidelines.

LSE's networks, computers, internet usage and email usage may be monitored and logged for all lawful purposes including:

1. Tracking the flow of network traffic
2. Facilitating and improving capacity planning
3. Identifying areas for improvement, including provision of teaching and learning facilities
4. Maintaining good availability of network bandwidth
5. Ensuring use of resources is authorised
6. Management of systems
7. Protecting against unauthorised access
8. Ensuring system security
9. Compliance with LSE policies and regulations and any other appropriate regulations all LSE users must comply with (e.g. the Joint Academic Network [JANET] [Acceptable Use Policy](#))
10. Avoiding or mitigating legal liabilities and complying with legal obligations
11. Preventing and detecting crime

Monitoring will include active attacks by users authorised by the LSE to test or verify the security of its systems.

During monitoring, information may be examined, recorded, copied and used for authorised purposes.

All information, including personal information, placed on or sent over LSE systems may be monitored.

During the monitoring process, personal data may be inadvertently seen or accessed by staff authorised to perform monitoring.

Monitoring will be automated in the detection and removal of viruses, malware, spam, pornography, inappropriate content and other activities not lawful to LSE business.

3.2 Email scanning

Incoming e-mail will be scanned by LSE mail filtering system. This includes using virus-checking software.

The software may block unsolicited marketing e-mail (spam), e-mail which has potentially inappropriate content or unscannable attachments, e-mail which breaks any legal or contractual agreement held by LSE or which contains any other inappropriate material.

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

3.3 Consent

Use of LSE information technology, authorised or unauthorised, constitutes consent by the user to the monitoring of these systems.

3.4 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 monitoring may be used subsequently in disciplinary, criminal or other proceedings.

3.5 Laws and regulations affecting LSE monitoring and logging

3.5.1 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

3.5.2 Data Protection Act 1998

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 Data Protection Act, to ensure personally-identifiable information is not made accessible outside of the identified groups in *Section 2* above. 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.

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

The Data Protection Act 1998 is available here:

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

3.5.3 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

3.5.4 Janet Acceptable Use Policy

LSE's internet service provider, Janet (the Joint Academic Network) requires that LSE is able to identify any person using the service.

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

3.5.5 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.

3.6 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.10.3.1 – Capacity Management: “The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.”

A.10.10 – Monitoring: “To detect unauthorized information processing activities” and including such processes as:

A.10.10.1: Audit logging: “Audit logs recording user activities, exceptions and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring”

A.10.10.2: Monitoring system use: “Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly”

A.10.10.3: Protection of log information: “Logging facilities and log information shall be protected against tampering and unauthorized access.”

A.10.10.4: Administrator and operator logs: “System administrator and system operator activities shall be logged.”

A.10.10.5: Fault logging: “Faults shall be logged, analysed, and appropriate action taken.”

3.7 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. All staff, students and any third parties authorised to access LSE’s network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

The below list of current policies is in no way authoritative and new policies will be published on the LSE website as they become available.

Associated policies:

[Information Security Policy](#)
[Anti-Virus Policy](#)
[Conditions of Use of IT Facilities at LSE](#)
[Conditions of use of the residences network](#)
[Password Policy](#)
[Asset Management Policy](#)
Data Protection Policy

Standards and Guidelines:

[Information Classification Standard](#)
[Encryption Guidelines](#)
[Remote and Mobile Working Guidelines](#)
[Guidelines on the use of Cloud storage](#)

3.8 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IT Services 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.