London School of Economics & Political Science

IMT

Procedure

Logging duration

Jethro Perkins
Information Security Manager

Version	Release 1.2
Date	17 September 2013
Library reference	ISM-PD-102

Table of contents

1 Introduction 3

1.1 Purpose 3
1.2 Scope 3

2 Responsibilities 4

3 Standard 5

3.1 Logs containing personal data or sensitive personal data 5
3.2 Logs that do not contain personally-identifying data 5
3.3 Time conventions 5
3.4 Legal and Regulatory Compliance 5
3.5 ISO27001 Controls 5

1 Introduction

The use of monitoring and logging IT systems and networks is mandated and explained in LSE's Monitoring and Logging Policy.

Collecting logs is a powerful tool in order to:

1. Track the flow of network traffic
2. Facilitate and improve capacity planning
3. Identifying areas for improvement, including provision of teaching and learning facilities
4. Maintain good availability of network bandwidth
5. Ensure use of resources is authorised
6. Manage systems
7. Protect against unauthorised access
8. Ensure system security
9. Comply 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. Avoid or mitigate legal liabilities and comply with legal obligations
11. Prevent and detect crime

Logs containing personally-identifiable data should only be held for the minimum possible time before being deleted.

1.1 Purpose

This standard lays out the minimum and maximum amounts of time different types of logs should be retained.

1.2 Scope

All LSE systems and networks.

2 Responsibilities

IMT
Responsible for most LSE servers, systems and networks.

Library IT Team
Responsible for library systems.

STICERD IT Team
Responsible for STICERD IT systems

IMT Information Security Team
Responsible for Monitoring and Logging Policy and all resultant standards.

3 Standard

3.1 Logs containing personal data or sensitive personal data

Any logs that contain personally-identifying data, Data Protection Act-defined *personal data* or *sensitive personal data*, or else contain LSE-defined *confidential* information, must be deleted after 3 months.

LSE's Information Classification Standard provides guidelines on evaluating the sensitivity and confidentiality of data.

3.2 Logs that do not contain personally-identifying data

Logs that do not contain any personally-identifying data may be kept indefinitely, as storage and operational requirements dictate.

3.3 Time conventions

Logs shall be recorded using UTC (Coordinated Universal Time).

3.4 Legal and Regulatory Compliance

Logs are kept and deleted in accordance with the following legal and regulatory requirements:

Computer Misuse Act 1990

Data Protection Act 1998

Regulation of Investigatory Powers Act 2000

Terrorism Act 2006

JANET Acceptable Use Policy

3.5 ISO27001 Controls

A.10.1.1 Documented operating procedures

A.10.7.3 Information handling procedures

A.10.10.1 Audit logging

A.10.10.3 Protection of log information

A.10.10.6 Clock synchronization