



London School of Economics & Political Science

IMT

Policy

Application Control

Jethro Perkins

Information Security Manager

Summary	This document outlines IMT's application control policy, as endorsed by December 2013 Information Technology Committee
Version	Release 1.0
Date	17/03/14
Library reference	ISM-PY-115

Document control

External document references

Title	Version	Date	Author
Information Security Policy	3	12/03/13	Jethro Perkins
Conditions of Use of IT Facilities	2.2	13/03/13	Jethro Perkins
Janet Acceptable Use Policy	11	May 2011	

Version history

Date	Version	Comments
17/03/14	1.0	Initial version, adapted into policy format from the paper presented to, and endorsed by, the December 2013 Information Technology Committee

Review control

Reviewer	Section	Comments	Actions agreed

Table of contents

1	Introduction	4
1.1	Purpose	4
1.2	Scope	4
2	Responsibilities	5
3	Policy.....	6
3.1	By default, applications will be whitelisted	6
3.2	Maintaining legitimate access to applications	6
3.3	Compliance, Policy Awareness and Disciplinary Procedures.....	6
3.4	Further Policies, Codes of Practice, Procedures and Guidelines	6
3.5	Review and Development	6
3.6	ISO27001 controls governing the LSE use of Application Blocking	6
4	Appendix A	8

1 Introduction

Whilst most applications developed for PCs and Macs are not malicious and do not of themselves threaten the confidentiality, integrity or availability of LSE data, there are a number of applications that are by their nature malicious, can be used to hack LSE systems or sniff LSE passwords and other confidential data.

There are also applications that are conduits or Trojans for malware, or provide easy routes for the transit of data into environments that have no guarantees of confidentiality, integrity or availability.

Other applications break LSE's '[Conditions of Use of IT Facilities](#)' and the [Janet Acceptable Use Policy](#) or LSE's legal obligations (for instance, the Data Protection Act 1998, Copyright Act 1988, Computer Misuse Act 1990, Protection of Children Act 1978, Sexual Offences Act 2003, Criminal Justice and Immigration Act 2008).

LSE must therefore be able to control the use of these applications, ensuring they are only used where and when it is appropriate.

1.1 Purpose

The primary purpose of this policy is to control the use of a minority of applications within the LSE environment as outlined above.

The purpose is not to block legitimate application access requirements that any member of the LSE community may have.

If anyone requests access to an application that has been blocked by Sophos, IMT will provide it upon written request to the Information Security Manager.

1.2 Scope

This policy applies to all devices owned by LSE or connected to LSE's network.

In the first instance application control will be managed by LSE's Sophos anti-virus console, and will be actively applied only to LSE's managed desktop estate.

Application traffic blocking will additionally be applied at the firewall level, when IMT has implemented its next generation firewalls.

2 Responsibilities

Members of LSE:

All members of LSE are responsible for acting within UK law and according to LSE's [Conditions of Use of IT Facilities](#) and JANET's Acceptable Use Policy.

All members of LSE are also responsible for reporting to the IMT Service Desk that an application has been blocked that they need to use.

IMT Service Desk

Responsible for accepting first line calls concerning application control.

IMT Networks

Responsible for implementing and maintaining application traffic blocking on the firewall.

IMT Information Security:

Responsible for managing application control via Sophos, maintaining the blacklist and whitelisting any used applications. Responsible for firewall-level blacklisting and whitelisting decisions for application traffic.

Information Security Advisory Board

Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee

Responsible for approving information security policies, including application control.

3 Policy

3.1 By default, applications will be whitelisted

Only a limited number of application categories will be blacklisted. These are listed in Appendix A

3.2 Maintaining legitimate access to applications

Legitimate application access requirements that any member of the LSE community may have will be maintained.

If anyone requests access to an application that has been blocked by Sophos, IMT will provide it upon written request to the Information Security Team. The request must outline the name of the application, who needs access and for what duration. The Information Security Manager will maintain a list of who has access to what resources and for how long. This list may be audited at any time and may be subject to disclosure resulting from a 'Freedom Of Information' request. If any student requires such access, they must ask an appropriate member of staff to request such access be enabled on their behalf.

3.3 Compliance, Policy Awareness and Disciplinary Procedures

Failing to comply with this policy, LSE's Conditions of Use of IT Facilities or Janet's AUP may result in criminal or civil action against LSE.

Any breach will be handled in accordance with all relevant School policies including HR's disciplinary processes.

3.4 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 via the [Information Security Policies, Procedures and Guidelines](#) page. 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.

3.5 Review and Development

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

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.

3.6 ISO27001 controls governing the LSE use of Application Blocking

A.7.1.3 Acceptable use of assets

- A.10.1.1 Documented Operating Procedures
- A.10.4.1 Controls against malicious code
- A.10.4.2 Controls against mobile code
- A.10.6.1 Network controls
- A.10.6.2 Security of network services
- A.11.4.1 Policy on the use of network services
- A.12.4.1 Control of operating software
- A.12.5.3 Restrictions on changes to software packages
- A.12.6.1 Control of technical vulnerabilities
- A.15.1.3 Protection of organizational records
- A.15.1.5 Prevention of misuse of information processing facilities
- A.15.2.1 Compliance with security policies and standards

4 Appendix A

Application Categories that contain programs that will be blocked. There may be individual programs within each category that are available for use.

Application vulnerabilities
Archive tool
Asset Management tool
Browser plug-in
Business Intelligence Tool
CRM tool
Design tool
Desktop search tool
Digital imaging
Distributed computing
Document viewer
Download manager
Email / PIM client
Encryption / Steganography tool
ERP Software
File sharing application
FTP Client
Game
Instant messenger client (IMC)
Internet browser
Jailbreak Software
Mapping application
Media conversion tool
Media player
Mobile Synchronization
Network monitoring / vulnerability tool
Office suite
Online storage
Optical burning tool
Optical Media Emulation
Password / license recovery tool
Pranking Software
Privacy tool
Programming / Scripting tool
Proxy / VPN tool
Remote management tool

Runtime Environment
Screen capture tool
Screensaver Application
Security / system tool
Security tool
Software updater
System tool
Telnet client
Tethered connection tool
Toolbar
USB Program launcher
Virtualization application
Voice-over IP (VoIP)