THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Technical

Anti-Virus Software on LSE computers

Introduction

The installation and use of anti-virus software and endpoint protection is a critical tool in LSE's defences against breaches of information confidentiality, integrity and availability. Whilst threats to information security have grown increasingly complex and difficult to detect, anti-virus software still provides a level of assurance against the most common and prevalent malware threats. Failure to install anti-virus software increases the risks not just to the confidentiality, integrity and availability of data and user information held on a machine, but also to those hosted on all other machines across the LSE network.

Purpose

The purpose of this policy is to stipulate that anti-virus software must be installed by default on all LSE-owned systems. Any required exceptions will be documented and communicated with the Cyber Security Team. Any machine connecting to the LSE network will be denied access if it is discovered to be not running anti-virus software.

Scope

- All LSE-built and managed systems (including servers, desktops, laptops and mobile devices), including non-DTS built and managed systems.
- All third party built and hosted systems used by LSE.
- End user devices (bring your own device) connecting to LSE's systems (for example by VPN) or otherwise on LSE's network.

Out of Scope

- Devices that are up-to-date and in support but that cannot run anti-virus software (e.g. things, door controllers, Apple phones and tablets.
- Unsupported legacy operating systems for which other arrangements are in place
- Systems in strict segregation from the rest of the LSE network, and with restricted outbound access only to the system supplier (e.g. point of sale devices)

Policy

- The anti-virus software supplied and managed by DTS must be installed, run and kept up to date as a default position on all systems owned and built by LSE, except for those considered out of scope (see above).

- All systems built and / or hosted by third parties that are used by LSE must run anti-virus software or display equivalent levels of security (file integrity monitoring software, SIEM reports and regular vulnerability assessment, for example).
- Any end user devices connecting to LSE's network by any means (VPN, wireless connection, wired connection).
- Unsupported legacy operating systems must use equivalent measures – e.g. access limitation via software firewalls and / or network segregation, file integrity checking, tripwire alerts etc.

Network Access

In order to maintain the security of LSE's network and protect the confidentiality, integrity and availability of data within it, DTS will deny any systems that are detected without up-to-date anti-virus and that do not meet the conditions above.

Exceptions

Any exceptions to the policy must be documented by the system owner and the appropriate remedial controls approved by LSE's Cyber Security team.

Apple mobile devices

Apple mobile devices (iPads and iPhones) cannot currently run anti-virus software. They are designed in such a way that each application has its own encrypted space that other applications cannot access, thereby preventing anti-virus scanning from functioning. Should this situation change and anti-virus software becomes available for Apple mobile devices, they will fall within the scope of this document.

Users of Apple mobile devices must keep their operating systems and applications up to date. Failure to do so will lead to these devices being blocked from LSE's network as security threats where they are detected.

Jailbroken Apple devices will be blocked from LSE's network as security threats where they are detected.

Problems

Any issues with installation, failure of anti-virus software to update, or other anti-virus related problems should be reported to the IT Service Desk (tech.support@lse.ac.uk)

Review schedule

Version:1.6 23/01/2024

Reviewed and approved by DTMB: 23/01/24 subject to amendments to v1.5 incorporated into v1.6

DTS reference: ISM-PY-111

Review interval	Next review due by	Next review start
3 years	Jan 2027	Nov 2026

Contacts

Position	Name	Email	Notes
Director of Cyber Security and Risk	Jethro Perkins	j.a.perkins@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	**Yes – website, regular messages via**

	Staff and Student News
Will training needs arise from this policy	**No**