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 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 exceptions will be documented. Any machine connecting to the LSE network may be denied access if it is 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.

Out of Scope

- Devices that cannot run anti-virus software (e.g. things, door controllers, Apple phones and tablets).
- Linux servers which are not required to host uploaded content or other user content that may contain malicious files.
- Systems in strict segregation from the rest of the LSE network, and with restricted outbound access only to the system supplier (e.g. tills)

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).

Network Access

In order to maintain the security of LSE's network and protect the confidentiality, integrity and availability of data within it, DTS may scan any system attached to the network for anti-virus software and may deny any systems without up-to-date anti-virus network access until such time that up-to-date anti-virus software is installed.

Exceptions

Any exceptions to the policy must be documented by the system owner and approved by LSE's Information 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 may lead to these devices being blocked from LSE's network as security threats.

Jailbroken Apple devices may be blocked from LSE's network as security threats.

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:1.4 22/09/2020

Reviewed and approved by IGMB: 16/11/20

DTS reference: ISM-PY-111

Review interval	Next review due by	Next review start
1 year	Oct 2021	July 2021

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?	**No**
Will training needs arise from this policy	**No**