

Policy

Anti-Virus Software on LSE computers

Jethro Perkins
Information Security Manager

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author

Version history

Date	Version	Comments
21/03/13	0.1	Initial version
23/04/13	1.0	Minor clarifications
10/06/13	1.1	Update to Section 3.2 (Exceptions) to further clarify the position of Apple mobile devices

Review control

Reviewer	Section	Comments	Actions agreed
10/06/13	3.2	Clarify the exception applied to Apple mobile devices (i.e. because they are designed in such a way that anti-virus software does not run)	Information Security Manager to update

Table of contents

1 Introduction..... 3
 1.1 Purpose..... 3
 1.2 Scope..... 3
2 Responsibilities 3
3 Policy 4
 3.1 Exceptions 4

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 documented and justified by the system owner. 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). All third party built and hosted systems used by LSE.

Responsibilities

IMT Systems Team

Responsible for installation of anti-virus software on servers and the standard desktop build.

IMT Support Teams

Responsible for the support and update of LSE workstations and laptops.

IMT Information Security Team

Responsible for approving or rejecting any suggested exceptions

LSE staff

Responsible for the update and maintenance of any mobile devices including Android phones and tablets.

LSE staff, students and third parties

Responsible for any user-owned devices brought onto campus or connected to the LSE network.

Policy

The anti-virus software supplied and managed by IMT must be installed, run and kept up to date as a default position on all systems owned and built by LSE.

All systems built and / or hosted by third parties that are used by LSE must run anti-virus software.

Details about LSE's anti-virus provision can be found at the following address:

<http://www2.lse.ac.uk/intranet/LSEServices/IMT/remote/protectYourOwnComputer/antivirusSoftware.aspx>

Network Access

In order to maintain the security of LSE's network and protect the confidentiality, integrity and availability of data within it, IMT may monitor 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 and justified by the system owner, recorded in LSE's Service Desk management software (currently Supportworks) and approved by LSE's Information Security team.

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.

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 (IT.Servicedesk@lse.ac.uk)

Review and Development

This policy shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly 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