Anti-Malware Policy

Owner:	
Approver (Date):	
Review due date:	March 2022
Current Version:	1.0
Update history:	N/A
Document Type:	Operational Policy
Classification:	Internal Only

To discuss receiving the document in an alternative format, please contact University Secretariat.

Contents

1. Introduction

1.1 The University of Roehampton has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services supplied by third parties but managed by the University of Roehampton.

1.2 The University has an obligation to provide appropriate and adequate protection of all its IT estate whether physical, virtual, on premise or in the Cloud.

1.3 Effective implementation of this policy reduces the likelihood of system compromise due to known vulnerabilities.

2. Scope

2.1 All IT systems owned by the University of Roehampton and managed by the University IT department, including hardware, software, mobile devices, USB storage media, mobile phones and tablets as well as any other peripherals

2.2 This policy applies to all employees, contractors, temporary workers and third parties who use, work with or connect to the University of Roehampton's computer network.

3. Responsibilities

3.1 The Chief Information Officer is accountable for ensuring that anti-malware software is installed on all computers connected or able to connect to the University of Roehampton's network

3.2 The IT Services Manager is responsible for ensuring that anti-malware software is installed, managed and maintained on all IT Systems connected to or able to connect to the University's computer network.

3.3 The IT Services Manager is responsible for monitoring software and systems for breaches of the anti-malware policy.

3.1 The University's IT department is responsible for ensuring that all anti-malware software they manage is maintained through regular software updates.

3.2 The University's IT department is responsible for ensuring that only white listed applications can be installed on University owned and managed mobile devices (smart phones and tablets)

3.3 The University's IT department is responsible for routinely assessing compliance with the anti-malware policy and will provide guidance to all the stakeholder groups in relation to issues of security and compliance.

3.4 Third Party Suppliers are responsible for ensuring that all IT systems they manage that connect to the University network and/or stores and processes University data assets have suitable anti-malware software installed and configured. Where this is not possible, this must be escalated to the Roehampton IT department.

3.5 All users of the University of Roehampton IT systems have responsibilities as defined in the Policy and regulations for the use of IT facilities and systems (2016)

4. Definitions

4.1 Malware is the common name given to software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

4.2 The University's IT department includes the Core Systems Manager, Solutions Analyst, Deputy Director IT and IT Security Manager.

4.3 IT Systems refers to:
- Physical Servers
- Virtual Servers
- Cloud hosted Servers
- End user compute devices (laptops/desktops etc.)
- Mobile devices (phones, tablets etc.)

5. Anti-Malware Policy

5.1 Anti-malware software is installed on all IT Systems and devices, including gateways and firewalls

5.2 The anti-malware software in use is configured to check for updates to its definition file automatically at least once a day.

5.3 All anti-malware software in use on University IT systems must be configured to:
- Scan files automatically upon access
- Scan removable media devices upon connection to a computer or other network device prior to files being accessed
- Perform scheduled scans of all local files
- Scan inbound and outbound email attachments
- Quarantine or delete suspect files
- Scan webpages when being accessed
- Prevent connections to known malicious websites

5.4 All University managed mobile devices are configured to limit the installation of applications through restricting them to approved applications delivered via the official Apple/Google Play store.

5.5 All approved applications are recorded in the University CMDB/MDM system

5.6 All exceptions to this configuration must be approved by the Chief Information Officer or their delegate.