UNIVERSITY OF EXETER

Anti-malware Policy

Version 2

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
1	June 17	Not known	New Policy
2	5/6/18	Ali Mitchell	New template

Review Distribution

Name	Title
Rhiannon Platt	Information Governance Manager and Data Protection Officer
Ian Tilsed	Assistant Director Strategy and Architecture

Approval

Name	Position	Signature	Date
	Members of the IGSSG		June 2017

1. Introduction

1.1 The University is obliged to make sure its IT systems and other facilities are secure and not subject to improper use. This Policy sets out the responsibilities of all users, including users of privately owned devices that connect to the University IT facilities, in relation to malicious software. These measures do not guarantee security, but they will help to significantly reduce the risk of widespread virus infection at the University.

1.2 The word ‘malware’ is used collectively to denote many types of malicious software, including viruses, ransomware, worms, trojans, macros, mail bombs and rootkits. A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user or business data.

1.3 There are many potential sources of malicious software, including websites, social media, USB memory sticks, unsolicited CDs, electronic mail, and software or documents copied over networks such as the campus network or the internet.

1.4 A malware infection is costly to the University and often time-consuming for individuals. This may be through the loss of data or access to IT systems, staff time to recover a system, or the delay or loss of important work. Additionally, malicious software can spread from an infected system and can lead to severe disruption to IT services and possible reputational damage or even fines. Malicious software is a constantly evolving threat and the University therefore applies controls to protect our systems and information from all forms of malware.

2. Scams and Hoaxes

2.1 Many spam emails are sent with dire warnings about messages with topical subjects or attachments. The receiver is often asked to forward the email to all colleagues and friends around the globe. If you are unsure whether an email you receive is a hoax or scam, you can check it at www.snopes.com. **Do not forward these messages on**. If you receive such a message, just delete it.

2.2 Some websites you visit will suggest your PC or tablet is infected with a new virus and hence you need to run / install / purchase their anti-virus software. **Do not click this message**. Instead, check that you have the latest signatures and updates in your existing anti-virus software and then run a manual scan.

2.3 If you download a fake anti-virus application, or think that your device has a virus, please report this to the helpdesk or to local IT staff as soon as possible, because it will be much easier to remove if reported promptly.

3. Scope

3.1 This Policy applies to all users, including ResNet users and other users of privately owned devices that connect to the University IT facilities. By following this Policy, users will help to protect themselves and other University users against malicious software. The University IT Regulations, on which this Policy expands, require everyone to take the practical steps needed to keep this protection active and up to date. If in doubt, contact the SID on sid@exeter.ac.uk extension 4724 or 0300 555 0444.

4. Purpose

4.1 The objectives of this document are:

- To set out user responsibilities about malicious software prevention
- To set out the rules governing the application and use of malicious software prevention systems at the University

5. Policy

- All University personal computers and servers that are connected to the University network or otherwise using the IT facilities must run an **approved** and **up-to-date** anti-malware product that continually monitors for malicious software (viruses, worms, etc.). Details of the approved products can be found at www.exeter.ac.uk/it/virusesandmalware

- All personal computers, devices and servers connected to the University network must run a supported version of the Operating System and installed applications with the latest available patches applied.

- Computers and tablets supported by Academic Services will be supplied with an anti-malware product with automatic updating for it and for the Operating System and applications.

- Any non-University owned devices must run an appropriate anti-malware product. Details of suitable products can be found at www.exeter.ac.uk/it/virusesandmalware

- Users who do not choose a recommended anti-malware product must make their own adequate anti-malware protection arrangements for their privately owned devices that meets the requirements described here.

- Anti-malware must be configured for on-access scanning, including the downloading or opening of files, folders on removable or remote storage, and web page scanning.

- Anti-malware protection software must be configured to run regular (at least daily) scans.

- Users must be prevented from accessing known malicious web sites either by malware protection software or through a content filtering function.

- Do not try to uninstall or disable anti-virus software. Any messages suggesting that anti-virus protection has been disabled should be investigated immediately.

- If users experience difficulties with a recommended anti-virus product, requests for technical support may be made through the helpdesk.

- The University's IT Regulations prohibit any activity intended to create and / or distribute malicious code (viruses, worms, etc) on the University network or IT facilities. However, when requested to do so by Exeter IT staff in order to aid investigations, users may send suspected malware using a method that does not allow the malware to propagate / spread.

- The University reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.

- If you suspect that a device is infected with a virus, report the incident to the helpdesk and / or to local IT staff as soon as possible.

- Email attachments must be scanned by an anti-virus product before delivery.

- Check the authenticity of attachments / software to be installed from internet sources. Do not install applications that arrive on unsolicited media.

Individuals may be subject to disciplinary action if this Policy is breached.