Virus Management Policy

1. Background

Malicious software such as viruses, worms and trojan-horse programs can cause widespread damage to any computer systems that they can run on. Many examples of such software have the ability to replicate themselves across networks and cause damage to many other computer systems and data files. This can be very costly and embarrassing for the University. Therefore, it is imperative the University adopt, and rigorously adhere to, a comprehensive anti-virus strategy incorporating education, protection, detection, reaction and recovery measures to reduce the likelihood of a virus outbreak and to minimise potential damage.

2. Definitions

In the following text:

"Malicious software" means any software that is intended to harm computer systems or the data held on computer systems and includes viruses, worms and trojan-horses.

"Detection software" means any software that can detect and/or remove malicious software.

"Computer" means any computing device and includes servers, workstations, laptops and mobile devices

Personal Computer means any computer whether owned by the University or not that is used by a member of the University or a visitor to access University data except that which is intended to be publicly accessible.

"Computer media" includes but is not limited to devices and all forms of device connected to a computer system using wired or wireless technologies for the purposes of storage

3. Purpose

The purpose of this policy is to define responsibility for virus control and to ensure that University systems and data are protected from malicious software. The policy is also intended to ensure that the University's reputation is not damaged by the effects or transmission of malicious software. As a result of this policy, it is intended that:

Computers connected to the University data network will operate as intended

Document Control
Reference: Virus Management Policy
Issue No: 1
Issue Date: 19.06.2018
Author: Director of IT Services

without any disruptions due to malicious software;

Appropriate monitoring for virus outbreaks will take place;

Recovery measures will be in place so that computers that have been damaged by malicious software can be quickly restored to normal operation.

4. Scope

This policy covers:

All members of the University and all visitors to the University.

All University computers whether connected to the University Data Network or not regardless of whether they are managed by IT Services or not.

All computers brought to the University by visitors which are to be connected to the University data network.

All forms of computer media.

5. Policy Statement

Any activity which is intended to create or distribute malicious software using the University network or University computers is strictly prohibited.

The University will promote the widespread use of detection software to all members of the University and will provide appropriate information and guidelines about their correct use.

Any outbreak of malicious software on University computers must be reported to IT Services Help Desk.

Suitable detection software must be identified and available for all computers that run operating systems included in the document Conditions of Use policy.

Detection software must be updated regularly along with regular 'signature' files updating and immediately on notification of an announcement about malicious software.

IT Services will employ detection software on all centrally managed computers and ensure it is active at all times.

Visitors to the University must ensure that all computers they use in the University have detection software installed on them which is operational and in accordance with this policy.

The University will provide students in the Halls of Residence with access to the latest versions of the standard detection software.

Students in Halls of Residence are allowed to connect a privately owned computer to the Residences network only if detection software is installed and in accordance with this policy.

Students in Halls of Residence with computers that run operating systems not in accordance with the document 'Conditions of use of computers and networks' must obtain their own detection software; ensure that it is regularly updated and is in accordance with this policy.

All files copied to computers used in the University must be checked for malicious software before being used. This includes files copied from magnetic media or files copied using technologies such as Infra Red, Bluetooth and wireless networks.

All members of the University must obey instructions given by IT Services in relation to malicious software or detection software.

6. Responsibilities

The Director of IT Services is responsible for reviewing this policy and for developing a corporate approach to detection software and procedures.

IT Services is responsible for selecting suitable detection software and making it available to all members of the University.

IT Services is responsible for scanning all incoming and outgoing electronic mail handled by the University e-mail service.

IT Services is responsible for ensuring that this policy is implemented on all centrally managed computers.

All members of the University are responsible for ensuring that client detection software is:

a. not deleted or uninstalled from PCs or devices;
b. is operating properly;
d. is not prevented from working or removed.

All members of the University are responsible for ensuring that any computer media introduced on to University computers does not contain any malicious software by checking the media using appropriate detection software as soon as the media is introduced.

7. Contacts

The IT Services Help Desk should be contacted in connection with any suspected outbreak of malicious software or for any other information about malicious software or detection software.

8. Sanctions

If a computer is known to be infected by malicious software it will be removed from the University network until it has been successfully disinfected and/or quarantined. IT Services support staff can assist individuals with recovery from infections, and the steps taken will include containment, disinfecting the system and capture of relevant incident information.

The sanctions given in the Code of Conduct in the acceptable use policy and the Use of IT Facilities apply to breaches of this policy.

9. Further Information

- General Conditions of Use of Computing and Network Facilities
- Data Protection Policy
- Information Security Policy
- BYOD Policy
- Wireless Networking Policy
- (JISC) JANET acceptable use policy