ANTI VIRUS POLICY

Document Id	Anti Virus Policy
Sponsor	Frank Briggs
Author	Jane Campbell, Nigel Rata
Date	May 2014

Version Control Log

Version	Date	Change
1.0	2/11/10	Initial draft for review
1.1	08/03/11	Updated
1.1	03/11	Approved
1.2	02/2013	Annual review and update
1.3	05/2014	Annual review and update

Document Approval

Name	Approval Signature	Approval Date
Frank Briggs	Approved	27.5.14
ITUAG	Approved	27.5.14

Introduction

A virus is a piece of self-replicating code, most often a malicious software programme designed to destroy or corrupt information, steal user data or adversely impact the usage of IT systems.

Potential sources of viruses include shared media such as USB memory sticks, electronic mail (including, but not limited to, files attached to messages), malicious code embedded in websites and software or documents copied over networks such as the internal network or the internet.

An infection by malicious software is almost always costly to the College whether through the loss of data, staff time to recover a system or the delay of important work. In addition, viruses spread from the College could potentially lead to serious issues of damage to reputation and possible litigation.

Scope

This document describes the measures taken by RHUL to counter malicious software and the responsibilities of individuals, departments and IT Services in protecting RHUL against viruses.

Anti Virus Policy

- All computers connected to the RHUL network must run an approved, licensed and up-to-date anti-virus product that continually monitors for malicious software.
- Currently all domain based, centrally managed computers must run the centrally managed virus protection software.
- Privately owned computers that connect to the college network must be equipped with an appropriate anti virus product.
- The College reserves the right to disconnect any machine from the network if an infection is found or suspected. The machine will remain disconnected until the infection is removed.

IT Service's Responsibilities

- IT Services will provide virus protection software for PCs and Macs. Due regard will be given to value for money and to providing a free or cheap version for use on personally owned staff and student machines. Software on the market at present usually provides anti-virus applications within a suite that has many other security features.

  Currently (Nov 2010)

  - IT Services has a site license for the Kaspersky Anti Virus suite. This software is deployed to all domain based Windows PCs.
  - Kaspersky Anti Virus is available for Mac as an individual machine download.
  - Kaspersky Anti Virus will be available for Linux systems in the future.

- Kaspersky Internet Security is available for staff and students to download free of charge on personally owned machines.
- RHUL central IT Windows Servers must run either ESet NOD32 security suite or Microsoft System Centre Endpoint Protection (SCEP). These are centrally managed antivirus products. The department made a strategic decision to separate out security software between the desktop, server and e-mail systems estate.
- The Unix/Linux estate security is currently managed by file and user permissions with a strong hardening policy.

Departmental Responsibilities

- All departments (whether managed by local IT-staff or central IT) must be protected by the centrally managed Kaspersky software suite for domain machines, and for non-domain machines the home (RHUL licensed) version of Kaspersky should be used.
- The IT department would recommend that all departmental Windows servers run the Eset NOD32 or Microsoft products. This can be provided via our centrally managed service. From May 2014 please check with IT Services as we are deprecating the NOD service.

Individual Responsibilities

- All staff and students are responsible for taking suitable measures to protect against virus infection.
- When using home computers to access RHUL resources remotely the computer must be protected by a suitable product. As a member of staff or a student you are entitled to a copy of the current security product purchased by IT on your home computing equipment.
- As the capabilities of mobile devices have increased and their use is becoming more widespread, these devices are being targeted more frequently by criminals. There are many potential sources of malicious software, including websites, social media, shared flash drives, unsolicited memory cards, and electronic mail accessed over networks such as the campus network or the internet. You should protect your device, and your personal and University data, against malicious activities. By default many mobile devices offer local encryption and browser-based phishing and malware detection, but some do not, so it is worth taking the time to become familiar with the security functionality on your device.

This policy will be reviewed on an annual basis and be tabled for approval with ITUAG.