

POLICY TITLE: Computer Virus Policy
POLICY #: IT - 6
DATE DRAFTED: December 05, 2005
APPROVED DATE: January 27, 2006
REVISION DATE:

1.0 Introduction

Viruses can infect Information Technology systems by a wide variety of methods including email messages, the Internet and through accessing infecting files contained on USB drives, floppy disks, CDs, and DVDs. Viruses can propagate very quickly as they are easily spread to other computers connected to a computer network, be it the TVCC network or the Internet.

It is vitally important therefore that any computer connected to the network has anti-virus software installed and that this protective software is kept current. Viruses can also attack vulnerabilities in applications such as Microsoft Office and operating systems such as Windows and this software must also be made secure by the application of critical patches and updates as and when required.

In order to combat viruses on the email gateway, servers and personal computing systems, the College has adopted a suite of system protection products from Symantec and Barracuda.

2.0 Purpose

This policy will clearly outline the responsibilities of Information Services and you, the User. Only by everyone recognizing their responsibilities will the risks to our networked infrastructure be minimized.

3.0 Policies

3.1. General

- All computer devices connected to the TVCC network or networked resources shall have anti-virus software installed, configured so that the virus definition files are current, routinely and automatically updated, and the anti-virus software must be actively running on these devices.
- All files on computer devices will be scanned periodically for viruses. IT Services will establish a schedule for automatically scanning the devices within their control.
- If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the network until the infection has been removed. This will be done under the direction of the Dean of Information Technology Services.

3.2. Information Technology Services' Responsibilities

- To ensure the agent software is installed on all IT managed servers and PCs.
- To ensure that all IT Services managed servers and PCs connected by the network are monitored, via the agent software, to maximize protection.
- To ensure that the latest anti-virus updates are made available in a central repository for scheduled non intrusive download by all managed network-connected servers and PCs.
- To ensure all ITS managed PCs, that are powered up and connected to the network, are fully scanned for viruses every Thursday evening.
- To ensure that security vulnerabilities are addressed on all locally installed or centrally delivered ITS approved software.
- To ensure that ITS managed servers and personal computing systems can be accessed remotely, as required.

3.3. Users' Responsibilities.

- Users must not prevent anti-virus updates being applied to their ITS managed PC.
- Users must not disable the anti-virus software on their ITS managed PC.
- Users must allow regular updates of software patches to their networked PC and restart their systems at least once a week.
- Users who connect to the college's University network from home or connect to the college through TVWireless with their own PC or laptop are responsible for ensuring their anti-virus software is up to date.
- Users should notify the ITS Helpdesk at 903-670-2621 immediately if they suspect a virus is present on any PC connected to the network.

3.4. In the Event of a Virus Outbreak.

- Information Technology Services will ensure that appropriate measures are taken at the earliest opportunity to minimize the risk of a virus outbreak.
- Information Technology Services will ensure that users are notified of a virus outbreak at the earliest opportunity using appropriate methods. This notification will offer advice to the user on how the virus risk can be

minimized and will outline any measures being taken by Information Technology Services in response to the available information.

- Information Technology Services will administratively disconnect a PC from the network, with little or no notice, to minimize the propagation of a virus or if the PC is deemed to be a security risk.
- Information Technology Services will require unhindered access (either remotely or locally) to any ITS managed network-connected PC to apply updates to software to minimize the risk of a virus outbreak or to repair critical security vulnerability.