Overview

Viruses, worms, and trojans have been responsible for a large percent of the security problems suffered by University computers. Most of these exploits can be prevented by the deployment of up to date and well maintained anti-virus software. The University subscribes to a service that provides anti-virus software and current virus definition file updates for every computer on the UT campus including some used for working at home.

Purpose

To ensure effective virus detection and prevention by establishing requirements which must be met by all computers connected to the University network

Scope

The anti-virus policy applies to all those who use University information resources including, but not limited to, faculty, staff, students, alumni, retired staff, contractors, consultants, guests, temporary staff, and other workers including personnel affiliated with third parties. The policy applies to all interactions with computing equipment associated with the business of the University and its projects. Some items do not apply to employees whose job definition requires these activities.

Policy

1. All network connected servers, workstations, and other hosts must run the University standard anti-virus software with the current definition files or an alternative application approved by Information Technology Services.

   All email servers shall run approved anti-virus software with current definition files installed to scan email messages for viruses before their being sent, received, and/or stored in a mailbox.

2. The University approved anti-virus software is configured for computers connected to the University network and therefore should retain the default configuration administered by Information Technology Services. Other approved anti-virus software must be configured to run or scan at regular intervals, upon receipt of an email or other files (real time virus scan), and by command to scan various types of media. The software must certify the computer to be virus, worm, and/or trojan free.

   If real time virus scan is available for an operating system, full disk scans should be done weekly at a minimum. If anti-virus software for an operating system does not include real time virus scans, full disk scans are necessary daily.

3. Servers, workstations, or other computing devices not complying with items 1 and 2 must not be attached to the UTHSC network or must be removed by the

user/administrator from the University network until they comply. This includes portable and non-portable devices regardless of the owner.

4. Servers, workstations, or other hosts that are infected with a virus, worm, and/or trojan must be removed by the user/administrator from the network until all evidence of the infection has been removed and the devices have been certified by Information Technology Services staff.

5. If a server, workstation, or other host is infected with a virus, worm, or trojan for which certified and reliable infection removing software is not available, the device's operating system and applications must be reinstalled from scratch and data or other user files must be restored from a cleaned or non-infected backup. The device must be certified by Information Technology Services staff before reconnecting it to the network.

Procedures

1.Always run the University standard, supported anti-virus software available from the University website: www.uthsc.edu/helpdesk select the section pertaining to antivirus.

2.Never open any files or macros attached to an email message from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately; also empty your trash to ensure removal.

3.Never download files or install applications from unknown or suspicious sources.

4.Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so. Any use of disk sharing should require passwords.

5.If you get media (floppy disks, CD's, zip disks, etc.) from another source, always scan them for viruses before using it or them.

6.As a safety measure back-up, critical data, system configurations, or other files you use on a regular basis in the event your computer is infected by a virus, worm, trojan or a computer failure. [Reference the **Backup Addendum**].

7.If software conflicts occur with the anti-virus software, run the anti-virus utility to ensure a clean computer, disable the anti-virus software, then run the conflicting software. Enable the anti-virus software after the task has completed. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

8.New viruses are discovered almost every day. Windows users receive virus definition updates automatically. Some operating system users do not receive file updates automatically. Users of these systems should, therefore, check periodically (ex. weekly) for new virus definition updates. The Help Desk can assist.

Enforcement

Reference **Enforcement** in the **Acceptable Use** document.

.

Additional Information

Any inquiries relating to this Anti-Virus Policy should be directed to the Security Director.