TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, **1.4.22 VIRUSES AND OTHER MALICIOUS CODE**

PURPOSE: To establish procedures that define the responsibilities for reducing the threat of computer viruses to TTUHSC El Paso computers and networks

To establish responsibility for overseeing computer virus prevention activities within TTUHSC El Paso, and to establish a reporting mechanism to ensure all appropriate personnel are contacted in case of a computer virus incident

To promote awareness of the threat posed by computer viruses to TTUHSC El Paso students, faculty, staff, and to ensure that virus protection software and procedures are properly implemented and utilized on a regular basis

REVIEW:

POLICY/PROCEDURE:

1. Due to the collaborative nature and sensitivity of the work performed at TTUHSC El Paso, all Institutional computers must have the institutionally provided antivirus software installed. Users' continued access to the TTUHSC El Paso network is contingent on the installation of institutionally provided antivirus software on all TTUHSC El Paso-owned computers. This virus protection software must not be disabled, bypassed, or modified in any way.
2. **Specific Restrictions**

TTUHSC El Paso expressly prohibits:

- Development of any form of computer virus with the intent to distribute through the TTUHSC El Paso network or beyond
- Intentional distribution of a virus, regardless of type (nuisance or destructive)
- Intentional creation of false alarms using hoax virus messages

3. **Specific Responsibilities and Guidelines for Virus Prevention**

Students, Faculty, and Staff should:

- Understand the risks associated with viruses and preventative measures that can be reasonably deployed.
- Be aware of and follow the procedures outlined in TTUHSC El Paso I.T. announcements (web page or email), which will be used to communicate warnings of potential computer virus threats.
- Treat nuisance viruses with the same urgency as destructive viruses. Write down the name of the virus, if provided by the virus detection software.

- Write down any recent unusual computer activities (for instance, unexpected disk access, error messages, or screen displays) and, if possible, include when these activities were first noticed.

- Contact the Information Technology Solutions Center when a computer virus is suspected and/or detected.

- Never boot directly from external devices or media until they have been scanned for viruses. By default, the Institutional antivirus program is configured to automatically scan all devices upon use. (This is completely done in the background without any visible disruption to the user.)

- Ensure files received from external sources are clean of viruses prior to use or distribution and never use or introduce non-licensed software on any TTUHSC El Paso computing device.

- Back up critical data (e.g., student/patient/employee information, data related to Institutional operations, vital mission data, etc.) to a floppy disk or to a drive on the server (see your Department Administrator or Departmental I.T. Representative for access restrictions) at least once a week (or more often for more critical data.)

4. Computer Security Analyst (CSA) is responsible for:

   - Isolating the infected computer(s) from the TTUHSC El Paso network as soon as possible. Reasonable attempts should be made to notify the primary user or the system administrator before disconnecting from the network. Depending on the nature of the virus, this may not be possible and the I.T. Solutions Center should be contacted prior to disconnecting a computer from the network. The Solutions Center will coordinate the ITS and networking to minimize any potential risks.

   - Identifying and isolating the suspected virus or worm-related file and processes. Do not power off or reboot computers that may be infected. There are some viruses that will destroy disk data if the computer is power-cycled or rebooted. Also, rebooting a computer could destroy needed information or evidence.

   - Attempt to halt and/or remove all suspicious processes from the computer. In the case of a worm attack, it may be necessary to keep the computer(s) isolated from the network until all TTUHSC El Paso computers have been inoculated and/or the other Internet sites have been cleaned and inoculated.

   - Implement fixes and/or patches to inoculate the computer(s) against further attack.

   - Notify the ITS prior to bringing the computers back into full operation mode. The users should also be notified the computers are returning to a fully operational state.

5. Information Technology Security (ITS)'s responsibilities include:

   - Overseeing computer virus protection activities within TTUHSC El Paso which include the desktops and servers, Internet mail gateway, and Exchange Servers. This is done in coordination with the CSAs.

   - Staying current with the latest virus exploits and maintaining attachment filtering lists through the mail servers.

   - Evaluating, recommending, and maintaining virus protection software and/or tools for use on TTUHSC El Paso PCs, servers, and laptops.

- Coordinating any training on virus control required for CSAs and TTUHSC El Paso personnel in general.

- Investigating every report of an apparent computer virus infection, and making every reasonable effort to determine the source of the infection. The Information Security Officer will keep all affected personnel advised of the investigation.

- Monitoring compliance of virus protection policies.

6. The CSA and ITS are jointly responsible for:

- Verifying the existence and identifying the type of virus on the user system.

- Coordinating with the anti-virus vendor or other sources on disinfection methods.

- Documenting any recent unusual computer activities (for instance, unexpected disk access, error messages, or screen displays) and, if possible, including when these activities were first noticed.

- Ensuring that the appropriate data for the monthly Department of Information Resources virus report is received by the Information Security Officer no later than the second business day of each month.

7. Information Technology PC Support/System Support should take the following steps:

- Ensure that virus protection software is installed on every desktop, server, and laptop computer acquired by TTUHSC El Paso before they are made available for use by TTUHSC El Paso students, staff, or faculty,

- Ensure that the virus protection software has loaded a 'terminate and stay resident' (TSR) program or service/daemon to constantly monitor for viruses to prevent introduction to the network,

- Inform the ITS/CSA of new anti-virus installs. This procedure is to make sure the desktop, server, or laptop can communicate with the anti-virus management server to receive updates,

- Upon receipt of a notice of a possible virus, clarify the symptoms with the user,

- Verify if there is a virus and if so, report the incident to the ITS/CSA, and

- In the event the virus cannot be removed from the infected computer, the ITS/CSA will contact PC Support or System Support to rebuild the computer.