	Information Security Policies and Procedures	No. COMP-Sec 3.3.1
	Title: MALICIOUS SOFTWARE PROTECTION PROCEDURE	Page: 1 of 3
		Revised Date: 12/22/04
		Original Date: 10/27/00

Malicious Software Protection Procedure

I. SCOPE

This procedure applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This Procedure applies to all Tenet information assets that provide access to data and all information asset Users.

II. PURPOSE

Provide guidelines for Tenet information asset Users regarding malicious software protection. Malicious software, including computer viruses, represents a real danger to the operational effectiveness of Tenet. The results of an infection can range from minor annoyance to complete system failure or total data loss. It is imperative that each Tenet information asset User follow procedures to safeguard against malicious software.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception shall be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

III. PROCEDURE


All Tenet information assets shall have a malicious software scanning tool activated. Users shall not disable or remove malicious software detection software from Tenet information assets.

A. Symptoms and Indications of Malicious Software, Including Viruses

Malicious software is any kind of software or code that could cause harm to the host or connected systems, and may include viruses, worms, and trojan horses. A computer virus is an unauthorized program that replicates and spreads through computing assets onto various data storage media (i.e. floppy disks, magnetic tapes, hard drives) and/or across a network, or resides in memory.

Symptoms of malicious software infection include, but are not limited to:

- a) Considerably slower computer response time;
- b) Unexpected and unexplained sending or receiving of e-mail messages;

	Information Security Policies and Procedures	No. COMP-Sec 3.3.1
	Title: MALICIOUS SOFTWARE PROTECTION PROCEDURE	Page: 2 of 3
		Revised Date: 12/22/04
		Original Date: 10/27/00

- c) Unexpected and unexplained Internet connections;
- d) Unexpected and unexplained loss of files;
- e) Changed modification dates for files;
- f) Stolen data from workstations, which could include PHI;
- g) Increased file sizes; and
- h) Total failure of computers.

B. Workstation Scanning


All workstations shall make use of the Tenet standard malicious software (including viruses) protection program.

- a) At boot-up, the malicious software detection program should check the file system and boot-up files;
- b) The malicious software protection program shall be resident in memory at all times;
- c) At a minimum, every computer (memory and files) shall be checked for malicious software on a weekly basis;
- d) All workstation malicious software scanning programs shall be set to scan "All" files, not just executables or program files; and
- e) The workstation malicious software scanning software shall be updated on a regular (weekly and when notified) basis.

C. Preventive Measures

All Users shall perform the following steps on a daily basis:

- a) All media (floppy disks, magnetic tapes, hard drives, etc.) shall be scanned for malicious software prior to using any of the files on the media or sending them to another party.
- b) All software and files downloaded from non-Tenet sources through the Internet

	Information Security Policies and Procedures	No. COMP-Sec 3.3.1
	Title: MALICIOUS SOFTWARE PROTECTION PROCEDURE	Page: 3 of 3
		Revised Date: 12/22/04
		Original Date: 10/27/00

(or any other public network) shall be screened with malicious software detection software. Screening of software and files shall take place prior to being opened or executed by another program such as a word processing package.

- c) All files that are received in a compressed state (“zipped”) or encrypted shall be scanned for malicious software before and after decompression or decryption.
- d) Apply all vendor security patches to protect workstations against known vulnerabilities.
- e) E-mail attachments shall be scanned for malicious software prior to opening.

D. Reporting Malicious Software

All Users must immediately report symptoms and indications of malicious software to the Information Systems Department.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- User Security Policy No. 3.0.0.
- Information Security Awareness Training Standard No. 3.2.0.
- User Conduct Standard No. 3.3.0.
- Malicious Software Control Procedure No. 8.2.4.