	Information Security Policies and Procedures	No. COMP-Sec 8.2.4
	Title: MALICIOUS SOFTWARE CONTROL PROCEDURE	Page: 1 of 3
		Revised Date: 12/22/04
		Original Date: 01/17/01

Malicious Software Control 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 and information asset Administrators.

II. PURPOSE

Provide direction for Tenet information asset Administrators regarding requirements for controlling malicious software. Tenet information assets may be susceptible to attack or infestation by malicious software from either internal or external sources. Malicious software infestation can lead to complete system shutdown.

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

Administrators of Tenet information assets shall configure those assets to resist and detect malicious software infection.

A. Standard Malicious Software Detection Software

The Tenet Information Systems Department has determined the appropriate commercially available malicious software (including virus) scanning software to be installed on information assets and facilities shall use the designated vendor’s product.

- a) The definition files shall be updated periodically (weekly) or when new malicious software threats are reported and supported by a new definition file.
- b) This software shall be updated whenever a new version or patch is released.
- c) An information asset that cannot be supported by the standard malicious software protection program shall be protected by one that can support it.

	Information Security Policies and Procedures	No. COMP-Sec 8.2.4
	Title: MALICIOUS SOFTWARE CONTROL PROCEDURE	Page: 2 of 3
		Revised Date: 12/22/04
		Original Date: 01/17/01

- d) Information assets that are vulnerable to malicious software attack or that store files for those systems that are vulnerable to attack, shall have a malicious software protection program active at all times.
- e) Disabling or removing malicious software detection software is prohibited.
- f) All software media shall be scanned for malicious software prior to installation.

B. Issuance of Warnings

A process for disseminating information related to malicious software shall be established at each facility.

- a) Malicious software shall be confirmed before warnings are issued.
- b) When informed that malicious software has been detected, each system administrator shall inform all Users with access to the same programs or data that malicious software may have infected their system.
 - (i) The Users shall be informed of the steps necessary to determine if their system has been infected and the steps to remove the malicious software.

C. Core Software Protection

Malicious software protection software shall be configured to monitor and protect operating system and application software running on workstations to prevent unauthorized modification.


D. Malicious Software Scanning Logs

Malicious Software scanning logs shall be recorded and made available for review when appropriate.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Malicious Software Protection Procedure No. 3.3.1.

	Information Security Policies and Procedures	No. COMP-Sec 8.2.4
	Title: MALICIOUS SOFTWARE CONTROL PROCEDURE	Page: 3 of 3
		Revised Date: 12/22/04
		Original Date: 01/17/01

- Technical Security Management Policy No. 8.0.0.
- Information Asset Administration Standard No. 8.2.0.
- Network Security Administration Standard No. 8.3.0 and its subordinate Procedures.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.