	Information Security Policies and Procedures	No. COMP-Sec 3.0.0
	Title: USER SECURITY POLICY	Page: 1 of 3
		Revised Date: 12/22/04
		Original Date: 10/26/00

User Security Policy

I. SCOPE

This policy 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 Policy applies to all Tenet information assets that provide access to data and all information asset Users.

II. PURPOSE

This Policy and associated Standards and Procedures define Tenet’s requirements for protecting *CONFIDENTIAL* and *PROPRIETARY* information by:


- a) Assuring information asset User access is granted to those with a need to know and limited by procedures establishing appropriate clearance and authorization;
- b) Providing information security awareness training to all information asset Users; and
- c) Establishing procedures and standards of User conduct concerning information assets.

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

III. POLICY

Tenet information asset Users will abide by the Information Security Policies and Procedures and other related Tenet standards and guidelines. Users will:

- a) Follow the Information Security Policies and Procedures for gaining access to and using Tenet information assets;
- b) Participate in the Information Security Awareness and Training program to ensure their understanding and compliance with the Information Security Policies and Procedures;
- c) Follow published Information Security Policies and Procedures; and

	Information Security Policies and Procedures	No. COMP-Sec 3.0.0
	Title: USER SECURITY POLICY	Page: 2 of 3
		Revised Date: 12/22/04
		Original Date: 10/26/00

d) Use Tenet information assets for business purposes.

A. User Privacy

Users shall not expect privacy with regard to Tenet’s information assets. Any e-mail, fax or voice-mail message that is created, sent, or received, and any file on the computer network, on local PCs, portable computers, or on disks located on Tenet property may be read or listened to at any time. *Every time a User logs on to these information assets, the User consents to such action.* Tenet expressly reserves the right to:

- a) Intercept, read, review, access, and disclose all e-mail messages;
- b) Intercept, read, review, access, and disclose all fax communications;
- c) Intercept, listen to, review, access, and disclose all voice-mail messages; and
- d) Intercept, read, review, access, and disclose all computer files including, but not limited to, Internet usage and websites that have been accessed.

Deleting e-mail messages and computer files does not necessarily mean there are no copies on the network or in storage, or that the information cannot be retrieved. It is possible Tenet could choose or be compelled to produce e-mail and computer files in litigation.

B. Background Checks


Background checks must be performed before employment at Tenet’s discretion.

- a) All contractors, agents, temporary workers, and other users who may have access to Tenet information assets must be screened in the same manner as employees of Tenet.
- b) Contractual agreements between Tenet and third party companies requiring this screening are sufficient for compliance with this policy.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.

	Information Security Policies and Procedures	No. COMP-Sec 3.0.0
	Title: USER SECURITY POLICY	Page: 3 of 3
		Revised Date: 12/22/04
		Original Date: 10/26/00

- Information Access Control Standard No. 3.1.0.
- Information Security Awareness Training Standard No. 3.2.0.
- User Conduct Standard No. 3.3.0.
- Tenet Human Resources Policies and Procedures No. 307-f “Employee Orientation”.
- Tenet Human Resources Policies and Procedures No. 401 “Employee Conduct and Work Rules”.
- Tenet Privacy Policies and Procedures No. 1.2.2 “Minimum Necessary”.