	Information Security Policies and Procedures	No. COMP-Sec 8.0.0
	Title: TECHNICAL SECURITY MANAGEMENT POLICY	Page: 1 of 4
		Revised Date: 01/11/06
		Original Date: 01/15/01

Technical Security Management 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 and information asset Administrators.

II. PURPOSE

Establish policies outlining Tenet’s directives for technical security management. There are three levels of technical security management required for Tenet information assets: network, system, and application.

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. POLICY

All information assets must be configured to support the concepts and instructions found in the Corporate Information Security Policies, Standards and Procedures.

Administrators of information assets that cannot support the policies and procedures must document the reason for non-support and indicate their alternate plan in their Information Security Control Exceptions Book.

A. Areas of Concentration


There are six major areas of information security that must be addressed by administrators of Tenet information assets. The content of each of these areas is described below.

1. Access Controls

These controls include provision of mechanisms that permit access by authorized individuals while preventing access by those not properly authorized.

2. Audit Controls

These controls consist of mechanisms employed to increase accountability by recording and supporting examination of system activity.

	Information Security Policies and Procedures	No. COMP-Sec 8.0.0
	Title: TECHNICAL SECURITY MANAGEMENT POLICY	Page: 2 of 4
		Revised Date: 01/11/06
		Original Date: 01/15/01

3. Authorization Controls

These controls include mechanisms for granting access to *CONFIDENTIAL* or *PROPRIETARY* information based on the individual's need-to-know as a requisite for performing their job.

4. Data Authentication Controls

These controls relate to the verification that information has not been altered or destroyed through unauthorized methods or access.

5. Entity Authentication Controls


These controls verify an entity and require the use of unique user identifiers, automatic logoffs, and a selection of other identifiers including biometrics, passwords, tokens or PINs.

6. Configuration Management Controls

These controls address the security of information systems in conjunction with the Information Security Policies and Procedures of the organization to create a coherent system of overall security. Configuration management includes:

- a) Documentation of all components of a system's security.
- b) Written procedures for connecting new hardware and software.
- c) Periodic review of system maintenance records.
- d) Periodic testing of the security attributes of the system.
- e) Maintenance of accurate documented inventory records.
- f) Security testing of systems including functional and penetration testing and verification.
- g) Virus checking.

B. Accomplishing Security Goals

	Information Security Policies and Procedures	No. COMP-Sec 8.0.0
	Title: TECHNICAL SECURITY MANAGEMENT POLICY	Page: 3 of 4
		Revised Date: 01/11/06
		Original Date: 01/15/01


Accomplishing Tenet’s security goals requires information asset Administrators to configure and manage information assets according to the Standards and Procedures subordinate to this policy. These Standards and Procedures include:

- a) Asset Access Controls Standard No. 8.1.0 provides direction for the management and configuration of UserID controls, password controls, and encryption controls.
- b) Information Asset Administration Standard No. 8.2.0 provides guidance and requirements for change control, auditing and logging procedures, virus control, and backup procedures.
- c) Network Security Administration Standard No. 8.3.0 provides direction regarding network security administration, network access controls, communications controls, and firewall administration.
- d) Operating System Security Standard No. 8.4.0 provides guidance for the security of the various operating system environments within Tenet.
- e) Application Security Administration Standard No. 8.5.0 provides direction for the security of applications in use at Tenet.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Physical Safeguards for Information Assets Policy No. 5.0.0 and its associated standards and procedures.
- Asset Access Control Standard No. 8.1.0.
- Information Asset Administration Standard No. 8.2.0.
- Network Security Administration Standard No. 8.3.0.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.
- Security Risk Management Standard No. 7.1.0.

	Information Security Policies and Procedures	No. COMP-Sec 8.0.0
	Title: TECHNICAL SECURITY MANAGEMENT POLICY	Page: 4 of 4
		Revised Date: 01/11/06
		Original Date: 01/15/01

- Tenet Administrative Policies and Procedures No. 2.1 “Capital Expenditure Review Process”.
- Tenet Administrative Policies and Procedures No. 2.18 “Coordination of Information Processing Systems”.