	Information Security Policies and Procedures	No. COMP-Sec 8.3.0
	Title: NETWORK SECURITY ADMINISTRATION STANDARD	Page: 1 of 3
		Revised Date: 12/22/04
		Original Date: 12/18/00

Network Security Administration Standard

I. SCOPE

This standard 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 standard applies to all Tenet information assets and information asset Administrators.

II. PURPOSE

Define standards of network operation and management that provide a stable and secure network environment. The network systems used by Tenet to connect computing assets are critical to the company’s business.

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. STANDARD

Networks, systems, and devices connected to Tenet networking assets shall be administered, configured, protected and monitored in accordance with this Standard and the supporting Procedures.

A. Network Responsibility


Tenet networks are currently provided and administered by a combination of a third party vendor and internal Tenet personnel.

1. THIRD PARTY VENDOR

A third party vendor provides the Wide Area Network (WAN) and some of the Local Area Networks (LAN) that form the backbone of the Tenet networks. The third party vendor is therefore the primary provider. The facility should enter into a Business Associate Agreement (BAA) with any third parties who meet the criteria of a business associate (see Information Handling Procedure No. 2.1.1 and Privacy Policies and Procedure No. 1.1.1 “Business Associates”).

2. TENET FACILITIES

Tenet facility LANs may be provided locally or by the third party. Any locally provided LANs shall meet all Information Security Policies and Procedures that

	Information Security Policies and Procedures	No. COMP-Sec 8.3.0
	Title: NETWORK SECURITY ADMINISTRATION STANDARD	Page: 2 of 3
		Revised Date: 12/22/04
		Original Date: 12/18/00

apply to their environment. The facility should enter into a Business Associate Agreement (BAA) with any third parties who meet the criteria of a business associate (see Information Handling Procedure No. 2.1.1 and Privacy Policies and Procedure No. 1.1.1 “Business Associates”).

B. Centralized Control

Additions, deletions, upgrades and changes to the Tenet network shall be controlled in a central location.

C. Compliance

Information assets may not be able to implement or support the Information Security Policies and Procedures as written. System Administrators shall configure the information assets to support the policies to the maximum extent possible. Compensating controls shall be implemented and documentation shall be maintained for those assets that cannot support the Information Security Policies. This documentation shall be maintained in the facility’s Information Security Control Exceptions Book and updated by facility management.

D. Standards of Common Carriers


The networking services at Tenet are provided on a contractual carrier basis, not those of a common carrier. Tenet operates a private network, and has the right to make policies that regulate the use of its network systems without being held to the standards of common carriers.

E. Service Provider of Public Network Services

Network assets shall not be used to provide services to non-Tenet entities outside of established contractual obligations. This includes operating as a public network or as a provider of services relied on by others. Examples include:

- a) A message forwarding node on the Internet.
- b) An encryption key notarization center or distribution point.
- c) A provider of information services.

F. Use of Evaluated Products

	Information Security Policies and Procedures	No. COMP-Sec 8.3.0
	Title: NETWORK SECURITY ADMINISTRATION STANDARD	Page: 3 of 3
		Revised Date: 12/22/04
		Original Date: 12/18/00

Essential functional requirements of Tenet networks shall be met through use of stable, proven hardware and software. Testing of new or unproven products shall not occur on Tenet production networks and systems.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Information Handling Procedure No. 2.1.1
- Information Asset Secured Area Protection Standard No. 5.1.0.
- Information Asset Open Area Protection Standard No. 5.2.0.
- Security Risk Management Standard No. 7.1.0.
- Technical Security Management Policy No. 8.0.0.
- Change Control Procedure No. 8.2.1.
- Network Security Administration Procedure No. 8.3.1.
- Network Access Controls Administration Procedure No. 8.3.2.
- Network Connections Procedure No. 8.3.3.
- Network Connection Safeguards Procedure No. 8.3.4.
- Transmission Security Procedure No. 8.3.6.
- Tenet Privacy Policies and Procedures No. 1.1.1 “Business Associates”.