	Information Security Policies and Procedures	No. COMP-Sec 8.3.2
	Title: NETWORK ACCESS CONTROLS ADMINISTRATION PROCEDURE	Page: 1 of 2
		Revised Date: 12/22/04
		Original Date: 12/18/00

Network Access Controls Administration 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 procedures that control access to Tenet’s network environment. A breach of network security may expose Tenet information assets to compromise and tampering. Access controls are key to preventing a breach of security.

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

A. Network Access

Tenet networks are provided for the use of authorized Tenet information asset Users, and network access should be provided accordingly.

B. User Access


User access should be provided in accordance with the Information Access Control Standard No. 3.1.0 and its subordinate procedures.

C. Administrative Access

Network Administrators may have access to various components of the network that are outside the control of the normal access request and granting channels. In those cases, Administrators shall develop their own procedures for granting access to those network assets using Information Access Controls Standard No. 3.1.0 as a guideline.

D. Control Packages for Connected Devices

Access to Tenet network and information assets shall be access controlled via an approved security application (the device operating system normally provides this application).

	Information Security Policies and Procedures	No. COMP-Sec 8.3.2
	Title: NETWORK ACCESS CONTROLS ADMINISTRATION PROCEDURE	Page: 2 of 2
		Revised Date: 12/22/04
		Original Date: 12/18/00

Users shall not be able to traverse from a network connection to a node (computer, router, or other asset) without going through a security protocol.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Information Access Control Standard No. 3.1.0 and its subordinate Procedures.
- Contingency Planning Policy No. 6.0.0 and its subordinate Standard and Procedure.
- Technical Security Management Policy No. 8.0.0.
- Asset Access Controls Standard No. 8.1.0 and its subordinate Procedures.
- Change Control Procedure No. 8.2.1.
- Logging and Auditing Procedure No. 8.2.2.
- Network Security Administration Standard No. 8.3.0.
- 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.