	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.1</b>
	<b>Title: NETWORK SECURITY ADMINISTRATION PROCEDURE</b>	<b>Page: 1 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/18/00</b>

**Network Security 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 network Administrators with procedures enabling compliance with Network Security Policies and Procedures. Standard administrative procedures shall be applied to all Tenet networks to ensure uniformity of security controls.

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**

Network Administrators shall apply consistent security controls on Tenet’s networks.

A. Internal Networks

Internal network devices and services can be accessed without transmitting through the public domain (i.e. dialup, internet).


1. Network Addresses are Proprietary

The internal addresses, configuration, and related system design information for Tenet networked information assets are proprietary and shall be restricted accordingly. Unauthorized Users shall not be able to use commands such as PING to obtain information about information assets connected to the internal network.

2. Avoidance Of Single Point Of Failure

Tenet networks shall be designed so that no single point of failure, such as a router or firewall, could cause network services to be unavailable.

B. Open or External Networks

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.1</b>
	<b>Title: NETWORK SECURITY ADMINISTRATION PROCEDURE</b>	<b>Page: 2 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/18/00</b>

The following controls shall be implemented to mitigate risks inherent to Internet or other external network usage:

1. External Network Connections

All external network connections shall comply with the Network Connection Procedure No. 8.3.3.

2. Malicious Software Scans

Software, data, files, E-mail messages, and other forms of information entering Tenet networks from outside sources shall be screened with malicious software detection tools. See the Malicious Software Protection Procedure No. 3.3.1 and the Malicious Software Control Procedure No. 8.2.4 for further information.

3. Alarms

Connection to an external network (i.e. the Internet) requires the monitoring of events on the open side of the Tenet firewall and alarms generated based on that monitoring.


- a) Alarming is defined as the real time (or near real time) notification of administrative staff of a potential breach of network access.
- b) If the firewall is incapable of this level of functionality, an intrusion detection system (IDS) shall be employed.

4. Audit Trail

Firewalls, intrusion detection systems, and authentication servers shall maintain audit trails of accesses and events. See the Logging and Auditing Procedure No. 8.2.2 for further details. Those audit trails shall be maintained with appropriate level of detail and for the appropriate length of time as determined by facility management.

5. Event Reporting

The physical elements of the network, especially those that are connected to the Internet, shall be monitored to ensure they have not been modified or compromised. See:

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.1</b>
	<b>Title:</b> <b>NETWORK SECURITY ADMINISTRATION PROCEDURE</b>	<b>Page: 3 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/18/00</b>

- a) Logging and Auditing Procedure No. 8.2.2.
- b) Change Control Procedure No. 8.2.1.

C. Operations

1. Implementation Of Security Problem Fixes

Security patches provided by operating system vendors, official computer emergency response teams (CERTs), and other trusted third parties shall be promptly implemented. All patches shall be proven reliable and free of defects or vulnerabilities prior to installation. Refer to the Change Control Procedure No. 8.2.1 for more information.

2. Command Access

Access to the operating system command (command prompt) shall be restricted. Users shall perform their work through menus or icons.

3. Use Of Diagnostic Test Hardware And Software

Diagnostic test hardware and software, such as communications line monitors, shall be used only by authorized personnel for testing and development purposes. Access to such hardware and software shall be strictly controlled.


4. Use Of Systems Software Utilities

Access to systems software utilities shall be restricted to a small number of trusted and authorized Users.

**IV. RELATED DOCUMENTS AND REFERENCES**

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Access Request and Modification Procedure No. 3.1.1.
- Malicious Software Protection Procedure No. 3.3.1.
- Contingency Planning Policy No. 6.0.0 and its subordinate Standard and Procedure.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.1</b>
	<b>Title:</b> <b>NETWORK SECURITY ADMINISTRATION PROCEDURE</b>	<b>Page: 4 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/18/00</b>

- 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.
- Backup Procedure No. 8.2.3.
- Malicious Software Control Procedure No. 8.2.4.
- 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 8.3.4.
- Transmission Security Procedure No. 8.3.6.