	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.3</b>
	<b>Title:</b> <b>NETWORK CONNECTIONS PROCEDURE</b>	<b>Page: 1 of 7</b>
		<b>Revised Date: 01/11/06</b>
		<b>Original Date: 12/18/00</b>

**Network Connections 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 guidelines for establishing connections to Tenet’s network environment. Connections to Tenet networks, whether internal or external, represent areas of potential information security vulnerability.

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. Trusted Network Configuration


The Tenet trusted network includes Local Area Networks (LANs), Wireless Local Area Networks (WLANs) and/or Wide Area Networks (WANs) that are entirely managed or owned by Tenet. Managed or owned includes physical and technical control of these networks, including access to and control of network equipment, wiring closets, cabling, hosts, information security, and network authentication capabilities. Components of the Tenet trusted network should be configured and controlled in accordance with Tenet Information Security Policies and Procedures.

The connection of LANs into the WAN is administered by a third party vendor. Connections to the WAN not administered by this third party vendor shall be approved by facility Management and the Corporate Information Systems Department.

B. Connecting Internal to External Systems

Precautions shall be taken to maintain the confidentiality, integrity, and availability of data when connecting internal to external (or external to internal) networks.

1. INTERNET CONNECTIONS

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.3</b>
	<b>Title:</b> <b>NETWORK CONNECTIONS PROCEDURE</b>	<b>Page: 2 of 7</b>
		<b>Revised Date: 01/11/06</b>
		<b>Original Date: 12/18/00</b>


Facility management and the Corporate Information Systems Department shall approve establishing Internet or any other external network connections that could allow non-Tenet Users to gain access to Tenet information assets.

- a) Tenet access to the Internet shall go through the corporate Internet portal as currently provided by the third party network vendor. Outside Internet Service Providers shall only be used with approval from the Corporate Information Systems Department.
- b) Connections between Tenet internal networks and the Internet (or any other publicly accessible computer network) shall include firewall and related access controls. See the Network Connection Safeguards Procedure No. 8.3.4.
- c) Users establishing a connection with Tenet information assets via the Internet shall authenticate themselves at a firewall or Remote Access Server (RAS) before gaining access to Tenet's internal network.

2. REMOTE (DIAL UP) ACCESS

Facility management shall approve dial-up modems connections that could allow access into or out of the trusted network.

- a) Users shall not connect dial-up modems directly to workstations or servers. Dial-up connections with Tenet information assets and networks shall be routed through a modem pool or remote access server to protect the trusted network and restrict dial-up users to only the required information assets.
- b) Strong User authentication systems are recommended to only provide dial-up users with access to the required information assets. UserIDs experiencing three (3) failed login attempts shall be disabled for fifteen (15) minutes to hinder potential password guessing attacks. UserIDs shall be locked out following three (3) consecutive disable cycles, and require an administrative reset.
- c) A virtual private network (VPN) should be used to protect data transmitted using a dial-up connection.
- d) Modems shall not be left in an “auto-answer” mode. The auto-answer mode enables the modem to receive in-coming dial-up calls. Modems should be configured for outgoing calls only or for dial back. If a modem must be configured to accept incoming calls, that modem should not answer until the

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.3</b>
	<b>Title:</b> <b>NETWORK CONNECTIONS PROCEDURE</b>	<b>Page: 3 of 7</b>
		<b>Revised Date: 01/11/06</b>
		<b>Original Date: 12/18/00</b>


fifth (5th) ring.

- e) It is recommended that devices with modems not be directly connected to the trusted network and a dial-up connection at the same time. This separation ensures that inadvertent access by an outsider is restricted to only the connecting device.
- f) It is recommended that dial-up modems be maintained in a disabled state when not in use. If possible, the third party requiring connection to the modem should request access through a hospital representative (i.e. hospital operator, help desk), the requestor should be authenticated, and the modem should be enabled for the amount of time required to perform the appropriate services.
- g) Information regarding access to Tenet computer and communication systems, such as dial-up modem telephone numbers, is considered *PROPRIETARY* information. This information shall NOT be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or otherwise made available to third parties. Individual voice telephone numbers, fax numbers, and Internet electronic mail addresses are permissible exceptions to this policy.

3. WIRELESS LOCAL AREA NETWORKS (WLANS)

Facility management and the Corporate Information Systems Department shall approve WLANS prior to implementation.

- a) Access points should support the IEEE 802.11b standard, and it is recommended that they support the 802.11g and/or 802.11i standards.
- b) WLANS shall be implemented so that no single point of failure would cause network services to be unavailable. Overlapping access points or reserve access points should be installed to provide this redundancy.
- c) Encryption shall be enabled on all WLANS to protect the confidentiality and integrity of transmissions of *CONFIDENTIAL* data.
  - (i) The 802.11i standard is recommended as the best option for providing data encryption for WLANS.
  - (ii) If the facility does not have the technology or cannot support the 802.11i standard, then Wi-Fi Protected Access (WPA) should be implemented


	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.3</b>
	<b>Title:</b> <b>NETWORK CONNECTIONS PROCEDURE</b>	<b>Page: 4 of 7</b>
		<b>Revised Date: 01/11/06</b>
		<b>Original Date: 12/18/00</b>

across the facility.

- (iii) If the facility cannot implement the 802.11i standard or WPA, then the Wireless Encryption Protocol should be implemented on all wireless access points.
- d) Authentication should be enabled on all WLANs to restrict wireless access to only authorized persons.
  - (i) Open system authentication (i.e. null authentication) is not permitted.
  - (ii) Extensible Authentication Protocol (EAP) is recommended as the best option for providing authentication.
  - (iii) Microsoft Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol Transport Layer Security (EAP-TLS) are acceptable alternatives for authentication.
  - (iv) If possible, credentials should be managed and verified against RADIUS, TACACS+, Active Directory or similar directories.
- e) Precautions should be taken ensure radio signal interference is not caused by WLAN implementation.
  - (i) Have the system installed by qualified professionals, who can complete a radio signal site survey prior to installation.
  - (ii) Use only properly certified components for the system.
- f) SSL VPNs eliminate the need for link-layer and network security schemes, and should be considered as a means for providing discreet connectivity.
- g) It is recommended that access to wireless access points be limited to only assigned MAC addresses.

C. Safeguarding Connections

Certain safeguards should be considered when connecting internal to external (or external to internal) networks.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.3</b>
	<b>Title:</b> <b>NETWORK CONNECTIONS PROCEDURE</b>	<b>Page: 5 of 7</b>
		<b>Revised Date: 01/11/06</b>
		<b>Original Date: 12/18/00</b>

1. FIREWALLS

Approved firewall(s), and/or other access control technology or processes shall be established between trusted and un-trusted networks. Firewalls should be established in accordance with the Network Connection Safeguards Procedure No. 8.3.4.

2. DE-MILITARIZED ZONES

De-Militarized Zones (DMZs) should be established to protect the trusted network from un-trusted networks that require access to an information asset, but not the entire trusted network. A DMZ should be considered when a third party requires access to a server (i.e. for maintenance, to install upgrades), but does not need access to the trusted network. DMZs should be established in accordance with the Network Connection Safeguards Procedure No. 8.3.4.

3. VIRTUAL PRIVATE NETWORKS

Virtual private networks (VPNs) should be established to protect information during transmission to/from, and remote access by, connected parties. VPNs should be established in accordance with the Network Connection Safeguards Procedure No. 8.3.4.

D. Other Network Connection Considerations


Other considerations should be made when providing third parties with connections into the trusted network.

1. NETWORK ADDRESS TRANSLATION

Unless otherwise specified, the details of the Tenet internal trusted network shall not be visible from outside the firewall. Network Address Translation (NAT) or Port Address Translation (PAT) shall be used to hide internal IP addresses (as described in best current practice RFC1918) from the outside world.

2. THIRD PARTY CONNECTION APPROVAL

The establishment of third party connections regardless of the method (Internet, public or private network), shall be approved by facility management and, where appropriate, the Corporate Information Systems Department.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.3</b>
	<b>Title:</b> <b>NETWORK CONNECTIONS PROCEDURE</b>	<b>Page: 6 of 7</b>
		<b>Revised Date: 01/11/06</b>
		<b>Original Date: 12/18/00</b>

3. RESPONSIBILITIES DEFINED FOR THIRD PARTY NETWORKS

Requests for access by third parties shall specify the security related responsibilities of Tenet and of the third parties. These responsibility statements shall address the liability exposures. All statements shall be in writing.

4. SECURITY REQUIREMENTS FOR THIRD PARTY NETWORKS


As a condition of gaining access to Tenet’s computer network, third parties shall secure their own connected systems in a manner consistent with Tenet requirements.

- a) Tenet shall include language in contracts with third parties providing the right to audit the security measures in effect on the connected systems.
- b) Tenet shall include language in contracts with third parties providing the right to terminate network connections with third parties not meeting Tenet security requirements.
- c) When appropriate, a Business Associate Agreement (BAA) shall be executed with third parties that are provided with access to protected health information (PHI) for the purpose of providing certain services on behalf of Tenet. See Information Handling Procedure No. 2.1.1 and Privacy Policies and Procedures No. 1.1.1 “Business Associates” for details.

**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.
- Technical Security Management Policy No. 8.0.0.
- Logging and Auditing Procedure No. 8.2.2.
- Network Security Administration Standard No. 8.3.0.
- Network Security Administration Procedure No. 8.3.1.
- Network Access Controls Administration Procedure No. 8.3.2.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.3.3</b>
	<b>Title:</b> <b>NETWORK CONNECTIONS PROCEDURE</b>	<b>Page: 7 of 7</b>
		<b>Revised Date: 01/11/06</b>
		<b>Original Date: 12/18/00</b>

- 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”.