	Information Security Policies and Procedures	No. COMP-Sec 8.1.0
	Title: ASSET ACCESS CONTROL STANDARD	Page: 1 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

Asset Access Control 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


Provide direction for administration and maintenance of access controls for Tenet information assets. Information asset access controls are used by Tenet to guard against risks to data integrity, confidentiality, and availability.

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

User access controls are required to secure access to Tenet information assets. At a minimum, user access controls must include a UserID and password. Access controls shall be put in place at the network (firewalls, network login) level, system (operating system) level, and when appropriate, at the application (database) level.

- a) Access controls shall be configured and administered in such a manner that the Information Security Policies and Procedures are supported. Administrators shall ensure they are familiar with all Information Security Policies and Procedures.
- b) The use of advanced technologies for identification and authentication can greatly enhance security over the standard UserID and password. The implementation of these technologies shall be coordinated with the Corporate Privacy/Security Office and Information Systems Department. These technologies include, but are not limited to:
 - (i) Tokens and Smart Cards;
 - (ii) Biometrics; and

	Information Security Policies and Procedures	No. COMP-Sec 8.1.0
	Title: ASSET ACCESS CONTROL STANDARD	Page: 2 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

(iii) Dial Back Modems.

- c) Tenet information assets shall not be open to “PUBLIC”, “GUEST” or “WORLD” access unless that information asset has been specified to allow public access.
- d) Programmers, administrators and other technical staff shall not install “back doors” that circumvent the authorized access control mechanisms found in operating systems and/or access control packages.

B. Automatic Logoff

All Tenet information assets shall be configured to automatically logoff inactive Users as appropriate for the environment. It is strongly recommended that automatic logoff occur after fifteen (15) minutes of inactivity, but the exact time settings should be determined by facility management. Considerations in establishing logoffs include:

- a) Length of inactivity until logoff;
- b) Provision of notification to the User;
- c) Documenting the logoff event;
- d) Impact on data and transaction processing; and
- e) Displaying a blank screen after logoff.


C. System Logon Banners

A system banner shall be presented to a User when the User attempts to logon to a network, system, or application. Banners shall include the following statement: “UNAUTHORIZED USE IS PROHIBITED”.

D. Reports

On at least a weekly basis, system administrators shall review security reports or other records of system activity (i.e. audit logs, access reports, security incident reports) to identify such events as:

- a) Changes in privilege levels;

	Information Security Policies and Procedures	No. COMP-Sec 8.1.0
	Title: ASSET ACCESS CONTROL STANDARD	Page: 3 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

- b) Emergency accesses as recorded in logs;
- c) Unusual use of privileges;
- d) Improper access attempts; and
- e) Failed logins.

Significant events identified through security report reviews should be reported to facility management.

E. Remote Access

Access to Tenet information assets from remote locations shall be restricted on an “as needed” basis. Any remote access connections should be established in accordance with Network Connections Procedure No. 8.3.3.


1. Restrictions For Vendor Support

Third party vendors who access Tenet information assets for support purposes shall have their access maintained in a disabled state until it is needed.

- a) When the access is required, it shall be enabled with an expiration of no more than 24 hours.
- b) Access shall be limited to the servers or services necessary for their tasks.
- c) General network access shall require facility management approval.
- d) Business Associate agreements (BAAs) shall be executed with vendors who are provided with access to protected health information (PHI) to perform their support.

2. Individual User Dial-Up Connections (Modems)

Users are prohibited from connecting dial-up modems to workstations without approval of the Corporate Information Systems Department. When a modem is authorized:

	Information Security Policies and Procedures	No. COMP-Sec 8.1.0
	Title: ASSET ACCESS CONTROL STANDARD	Page: 4 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

- a) It shall not be in auto-answer mode, such that it is able to receive in-coming dial-up calls.
- b) A workstation shall not be connected to a LAN (network connection) and a modem at the same time.

3. Systems Accepting In-Coming Dial-Up Calls


Communications systems that accept in-coming dial-up calls shall not be established unless these systems have first been approved by the facility Information Systems Department.

- a) Connections routed through a modem pool shall include an approved extended user authentication security system (such as a Remote Access Server (RAS)).
- b) Access points shall be isolated from the Tenet LAN/WAN environment by a firewall.
- c) If a remote User connecting via a dial-up line is unable to provide a correct password within a maximum of three (3) attempts, the connection shall be terminated.
- d) Remote UserIDs experiencing five (5) failed login attempts within a reasonable period (thirty (30) minutes is recommended) shall be disabled for some period (thirty (30) minutes is recommended) to hinder potential password - guessing attacks.
- e) Dial-up modems shall not answer in-coming calls until the fifth (5th) ring.

4. Dial-Up Access Numbers In Directories

Information regarding access to Tenet information assets and communication systems, such as dial-up modem telephone numbers, is considered PROPRIETARY.

- a) 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 without the advance written permission of facility Management.
- b) Telephone numbers, fax numbers, and Internet electronic mail addresses are permissible exceptions.

	Information Security Policies and Procedures	No. COMP-Sec 8.1.0
	Title: ASSET ACCESS CONTROL STANDARD	Page: 5 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Record Processing Policy No. 2.0.0 and its subordinate Standard and Procedure.
- User Security Policy No. 3.0.0 and its subordinate Standards and Procedures.
- Physical Safeguards for Information Assets Policy No. 5.0.0 and its associated Standards and Procedures.
- Technical Security Management Policy No. 8.0.0.
- UserID Control Procedure No. 8.1.1.
- Password Control Procedure No. 8.1.2.
- Encryption Control Procedure No. 8.1.3.
- Logging and Auditing Procedure No. 8.2.2.
- 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.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.