	Information Security Policies and Procedures	No. COMP-Sec 3.1.0
	Title: INFORMATION ACCESS CONTROLS STANDARD	Page: 1 of 4
		Revised Date: 12/22/04
		Original Date: 10/27/00

Information Access Controls 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 Users.

II. PURPOSE

Provide direction on the appropriate methods to protect the confidentiality, availability, and integrity of Tenet information assets through control of User access. The information Tenet uses and controls may be accessed via a variety of methods. The information might be displayed by an application, accessed via a PC or mainframe computer, printed for viewing or inclusion in a record or accessed via the Intranet. The owners and administrators of the information assets shall work together to establish appropriate levels of access for individual Users.

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 Controls Exception Book.

III. STANDARD

A. Access Types


1. Individual Access

Except as provided in Section III.B.1. of this policy, access to Tenet information assets is granted on a need to know basis, to specific individuals, not entire classifications of individuals.

- a) Each request for access shall be authorized by facility management or a delegate of facility management.
- b) All access to Tenet information assets shall be accomplished using a unique UserID that can be traced to one single User.

2. File and Directory Level Access

When sharing or assigning access to any file or directory containing Tenet *CONFIDENTIAL* or *PROPRIETARY* information, the access shall be restricted to

	Information Security Policies and Procedures	No. COMP-Sec 3.1.0
	Title: INFORMATION ACCESS CONTROLS STANDARD	Page: 2 of 4
		Revised Date: 12/22/04
		Original Date: 10/27/00

individual Users. Establishing file access to ALL Users requires facility management approval.

- a) Access shall be enforced at both the UserID level (privileges) and at the file level (access lists or file privilege settings).

3. Emergency Access

When an information security incident, disaster, or other emergent event occurs, access controls may have to be bypassed. Emergency Access to networks, systems or applications where *CONFIDENTIAL* or *PROPRIETARY* information may be exposed, can be granted only with the approval of Tenet Corporate or facility management (CEO, CFO, CIO).

- a) Any emergency access shall be logged, audited, and documented and a copy of that documentation shall be maintained at the facility.
- b) Emergency access rights shall be removed as soon as the emergency is concluded.
- c) Refer to Incident Handling Policy No. 4.0.0, Contingency Planning Policy No. 6.0.0 and the associated standard and procedure for further information.

B. Access Privileges


Access to Tenet information assets must be authorized.

1. Management Responsibility

Facility management shall approve specific written standards regarding the categories of people who are granted permission to access various types of information and reevaluate the privileges granted to all Users on all systems at least annually.

2. Revocation of Access Privileges

Facility management reserves the right to revoke the privileges of any User at any time. Conduct that interferes with the operation of Tenet information assets, which adversely affects the ability of others to use these information assets, or which is harmful or offensive to others is not permitted and may result in privilege revocation.

	Information Security Policies and Procedures	No. COMP-Sec 3.1.0
	Title: INFORMATION ACCESS CONTROLS STANDARD	Page: 3 of 4
		Revised Date: 12/22/04
		Original Date: 10/27/00

C. Unauthorized Access

Users of Tenet information assets are prohibited from gaining access to any information asset for which they are not authorized. Users are also prohibited from damaging, altering, or disrupting the operations of any information asset. Unless specifically authorized by facility management, Users are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access. Unauthorized access is considered cause for immediate disciplinary action, up to and including termination.


1. Information Asset Penetration Tools Prohibited

Unless specifically authorized by facility management, Tenet information asset Users shall not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or disrupt information assets. Examples of such tools include those that discover or ‘trap’ passwords, identify security vulnerabilities, or intercept or copy information. The unauthorized use or possession of tools of this nature is considered cause for immediate disciplinary action, up to and including termination.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- User Security Policy No. 3.0.0.
- Access Request and Modification Procedure No. 3.1.1.
- Access Termination Procedure No. 3.1.2.
- Technical, Maintenance and Housekeeping Personnel Access and Supervision Procedure No. 3.1.3.
- Sanctions Standard No. 4.1.0.
- Contingency Planning Policy No. 6.0.0.
- Contingency Planning Standard No. 6.1.0.
- Contingency Planning Procedure No. 6.1.1.

	Information Security Policies and Procedures	No. COMP-Sec 3.1.0
	Title: INFORMATION ACCESS CONTROLS STANDARD	Page: 4 of 4
		Revised Date: 12/22/04
		Original Date: 10/27/00

- Security Administration Policy No. 7.0.0.
- Asset Access Controls Standard No. 8.1.0.
- UserID Control Procedure No. 8.1.1.
- Password Control Procedure No. 8.1.2.
- Tenet Privacy Policies and Procedures No. 1.2.2 “Minimum Necessary Procedure”.