	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.0</b>
	<b>Title: INFORMATION ASSET ADMINISTRATION STANDARD</b>	<b>Page: 1 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/17/01</b>

**Information Asset Administration 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 of Tenet information assets. Information asset administration is a function that allows Tenet to maintain the control and security of information assets. Security issues shall be an active consideration in managing Tenet information assets.

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**

Effective administration of information assets requires implementation of adequate procedures, including:

- a) Change control (configuration management);
- b) Logging and auditing;
- c) Data backup;
- d) Malicious software controls; and
- e) Documentation.

A. Change Control

The security goal of change control is to assure that security of information assets is not compromised because of hardware or software changes. Facility management shall ensure that changes to Information Assets are reflected in the facility’s contingency plan.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.0</b>
	<b>Title: INFORMATION ASSET ADMINISTRATION STANDARD</b>	<b>Page: 2 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/17/01</b>

Certain procedures shall be followed in change control to minimize the likelihood of information security incidents. See Change Control Procedure No. 8.2.1 for further information.

**B. Logging and Auditing**

Logging and auditing are activities that support Tenet’s information security program by providing the ability to identify and assign accountability for the actions of an individual User.

- a) Data is logged by systems in the course of operation and, where possible, reports are produced summarizing various types of activities of individual Users.
- b) Audits are performed in which logs are reviewed at various intervals by managers and auditors from within a facility or other parts of Tenet. See Logging and Auditing Procedure No. 8.2.2 for further information.

**C. Data Backup**


Backups of critical information assets are a key aspect in assuring the confidentiality, integrity, and availability of Tenet information. Backups are performed by operations personnel and in some cases by Users. See the Backup Procedure No. 8.2.3 for further details. Considerations to include in planning backups include:

- a) Frequency of backups based on the frequency of changes to data;
- b) Criticality of the data;
- c) Usability of the backups; and
- d) Storage of backups in secure locations.

**D. Malicious Software Controls**

Potential malicious software in Tenet managed information assets requires using software that protects against infection, detects infection, and removes infection. See Malicious Software Control Procedure No. 8.2.4 for further information.

**E. Documentation**

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.0</b>
	<b>Title: INFORMATION ASSET ADMINISTRATION STANDARD</b>	<b>Page: 3 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/17/01</b>

Fully documented operations aid in reducing security problems arising from operational oversights, support training of staff, and provide measures for auditing operational effectiveness. Tenet facilities shall maintain documentation used in the administration of information assets including hardware, software, and operational procedures.

Documentation includes:

- a) Operating manuals;
- b) Processing procedures;
- c) Maintenance logs; and
- d) Configuration and settings standards.


All information assets used for Tenet business activities shall have sufficient documentation to ensure continued and consistent operations.

- a) Information assets shall be documented prior to deployment and whenever a change is made that would affect the accuracy of that documentation.
- b) The documentation shall be written so that the asset may be understood, run or reconfigured by persons unacquainted with the asset.

#### **IV. RELATED DOCUMENTS AND REFERENCES**

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Technical Security Management Policy No. 8.0.0.
- 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 and its subordinate procedures.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.0</b>
	<b>Title:</b> <b>INFORMATION ASSET ADMINISTRATION STANDARD</b>	<b>Page: 4 of 4</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/17/01</b>

- Operating System Security Standard No. 8.4.0 and its subordinate procedures.
- Application Security Administration Standard No. 8.5.0.