	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.1</b>
	<b>Title:</b> <b>CHANGE CONTROL PROCEDURE</b>	<b>Page: 1 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/15/01</b>

**Change Control 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 direction for Tenet information asset administrators regarding change controls. Change control (configuration management) is the method by which Tenet maintains control of changes to 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. PROCEDURE**


Modifications to, or additions or removals of, hardware (systems, networks, firewalls, etc.), software (operating systems, applications, programs, etc.), or other information assets in a Tenet production environment, shall be made in compliance with Tenet approved change control processes. Software development should comply with the information security steps outlined in the IEEE 12207.0 standard.

A. Hardware and Software Controls

As the unauthorized addition of hardware or software may inadvertently create vulnerabilities in the Tenet information asset environment or render archived media unrecoverable, all Tenet entities must follow approved processes for technology changes made to the Tenet production environment. These change controls procedures do not apply to test environments owned or managed by Tenet.

1. Hardware Controls

The hardware used at Tenet shall be properly accounted for using the following guidelines:


	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.1</b>
	<b>Title:</b> <b>CHANGE CONTROL PROCEDURE</b>	<b>Page: 2 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/15/01</b>

- a) All information asset hardware shall be inventoried on an annual basis (including non-capital items).
- b) A Tenet property sticker shall be applied to all hardware assets.
- c) Loss or theft of information assets shall be reported to site security and to Corporate Security Operations in accordance with Administrative Policies and Procedures No. 2.42 “Reporting of Theft of Assets and Property”.
- d) Loss or theft of information assets that may contain *CONFIDENTIAL* material shall be handled according to the Incident Handling Policy No. 4.0.0 and its subordinate standard and procedures.
- e) Microcomputer equipment (PCs, LAN servers, etc.) shall not be moved or relocated without the prior approval of the involved department manager.

2. Software Controls

The software used by Tenet information assets must be properly licensed according to the particular license agreements.

- a) Tenet shall comply with all legislation, laws and regulations concerning the licensing of the software used in Tenet’s business practices. This policy supports the User Security Policy No. 3.0.0 and its subordinate standards and procedures.
- b) License management software (provided by the Corporate Information Systems Department) shall be used to:
  - (i) Assist in detecting the addition of licensed software.
  - (ii) Assist in detecting new and/or modified application programs developed by end-users.
- c) A database of license information shall be maintained.
  - (i) All software licenses, whether paper or electronic, shall be maintained by the providing entity (corporate or facility).
  - (ii) Annual audits of software and software licenses shall be conducted.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.1</b>
	<b>Title:</b> <b>CHANGE CONTROL PROCEDURE</b>	<b>Page: 3 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/15/01</b>

(iii) Agreements for all computer programs licensed from third parties shall be periodically reviewed to ensure compliance.

(iv) Third party software shall be registered with the appropriate vendor.

d) Illegal copies of software shall be removed from Tenet information assets or the proper licenses for the software will be obtained.

**B. Changes to Information Assets**

Maintaining integrity of information requires application of change control principles. Change management processes shall be followed when:


- a) Installing software and security patches.
- b) Upgrading or downgrading software to another version.
- c) Increasing existing hardware capabilities and capacities.
- d) Replacing existing hardware.

**C. Elements of Change Control**

**1. Change Review Committee**

A review committee shall review and approve all changes to hardware and software that affect or have the potential of affecting the security, manner, cost, production, profitability, or any other aspect of business.

- a) Committee members shall review:
  - (i) New Applications (developed internally or purchased from third party).
  - (ii) Modifications to Existing Applications.
  - (iii) Operating Systems (changes, extensions, modifications, or replacements).
  - (iv) Hardware (Servers, firewalls, routers, etc).
- b) The review committee shall be appointed by the facility Information Systems Department, and should include representatives of user groups that could be


	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.1</b>
	<b>Title:</b> <b>CHANGE CONTROL PROCEDURE</b>	<b>Page: 4 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/15/01</b>

affected by the change to information assets.


2. Change Control Process

Steps in the change control process shall include:

- a) Proposed changes shall be presented to the review committee prior to the beginning of the development process.
  - (i) Security issues shall be discussed at this time, including:
    - (1) General security risks;
    - (2) Service interruption; and
    - (3) Compliance with the Tenet Information Security Policies and Procedures.
  - (ii) The committee will approve all development and testing plans.
- b) Complete Development
  - (i) Development staff shall not be permitted to access production data and systems that are not necessary for their current development and testing work.
  - (ii) Complete Testing (Refer to Application Security Administration Standard No. 8.5.0 for further information). Testing shall include, but is not limited to hands-on functional testing, penetration testing, and verification of the results. Whenever appropriate, Users shall be included on the testing team.
    - (1) Testing shall not be performed in a production environment.
      - a. Whenever possible, separation of testing and production environments shall be achieved via physically separate information systems.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.1</b>
	<b>Title:</b> <b>CHANGE CONTROL PROCEDURE</b>	<b>Page: 5 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/15/01</b>

- b. When computing facilities do not allow physical separation, logical separation (separate directories/libraries with strictly enforced access controls or firewalls) shall be employed.
  - (2) Data used for testing shall be:
    - a. Sanitized such that protected health information is sufficiently de-identified (scrambled or mismatched) to ensure confidentiality.
    - b. Treated with the same handling procedures that applied when it was production data.
    - c. Reviewed and authorized for use by the information custodian.
  - (3) Validate data prior to performing queries or updates on databases or any data repository. Employ parity checks, check-sums, and error detection data validation techniques.
- c) Review test results and implementation plan.
    - (i) The review committee shall evaluate the test results, review the proposed changes review the revised production schedule, and ensure that the back-out process is complete and tested before implementing the proposed change.
    - (ii) The review committee shall approve all implementations prior to their deployments.
  - d) When applying patches or similar software changes to a number of systems (i.e. servers, workstations), it is recommended that these changes be applied progressively from the least to the most critical information asset. This should assist in identifying implementation problems not discovered during testing prior to applying these changes to the facility's most critical information assets.
  - e) A post implementation review shall be conducted and the results presented to the review committee.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.1</b>
	<b>Title:</b> <b>CHANGE CONTROL PROCEDURE</b>	<b>Page: 6 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/15/01</b>

f) All pre and post implementation review results must be documented and stored in a secure location.

3. Movement Of Software From Development To Production


Certain controls shall be implemented before moving software from testing to the production environment, including:

- a) Development staff shall not move any software into the production-processing environment.
- b) Technical staff not associated with the testing process shall perform review and recompilation activities.
- c) Automatic updating of software on information assets via “push” technology shall be prohibited unless the involved software has first been tested.
- d) When vendor-testing processes are adequate, and when reliable vendor quality control measures exist, exceptions can be made.
- e) Adequate "back-out" procedures shall be developed and documented for all changes to production systems, applications or other information assets to allow the original configuration to be re-instated.
- f) Configuration information, applications and data back-ups of the target system shall be stored separately from the target system.

4. Movement Of Hardware and Electronic Media

Certain procedures shall be followed when moving hardware and electronic media including:

- a) A retrievable, exact copy of the information stored on the hardware and/or electronic media shall be created prior to movement of the equipment.
- b) Records of movements of hardware and electronic media shall be maintained by the responsible department. These records shall include a description of the equipment, the Tenet property sticker identification number, date and time of the movement, and person(s) responsible for the movement.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.2.1</b>
	<b>Title:</b> <b>CHANGE CONTROL PROCEDURE</b>	<b>Page: 7 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/15/01</b>

#### IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- User Security Policy No. 3.0.0 and its subordinate Standards and Procedures.
- Incident Handling Policy No. 4.0.0 and its subordinate Standard and Procedure.
- Technical Security Management Policy No. 8.0.0.
- Information Asset Administration Standard No. 8.2.1.
- Network Security Administration Standard No. 8.3.0 and its subordinate procedures.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.
- Tenet Administrative Policies and Procedures No. 2.1 “Capital Expenditure Review Process”.
- Tenet Administrative Policies and Procedures No. 2.18 “Coordination of Information Processing Systems”.
- Tenet Administrative Policies and Procedures No. 2.19 “Duplication of Personal Computer Software”.
- Tenet Administrative Policies and Procedures No. 2.42 “Reporting of Theft of Assets and Property”.