	Information Security Policies and Procedures	No. COMP-Sec 3.1.1
	Title: ACCESS REQUEST AND MODIFICATION PROCEDURE	Page: 1 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

Access Request and Modification 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 Users.

II. PURPOSE

The purpose of this document is to outline the procedures for adding or modifying User access to Tenet information assets. Granting or modifying access to Tenet information assets requires completion of procedures that ensure appropriate access is provided to each information asset User.


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. Management Responsibility

Facility management shall assign responsibility for controlling User access to Tenet information assets. Facility management’s responsibilities also include:

- a) Ensuring access is provided only to those Users that have a need to access Tenet Information assets and that such access is limited to the minimum necessary information for the user to perform required functions (see Privacy Policies and Procedures No. 1.2.2 “Minimum Necessary”);
- b) Ensuring the eID Security Request Form for Corporate managed systems (see URL attached hereto as Addendum “A”) is accurately completed and routing for processing;
- c) Ensuring a Security Request Form is developed and utilized for all information assets not administered by Corporate (see sample attached hereto as Addendum “B”);
- d) Ensuring requested User access does not conflict with the User’s job responsibilities or with previously assigned access;

	Information Security Policies and Procedures	No. COMP-Sec 3.1.1
	Title: ACCESS REQUEST AND MODIFICATION PROCEDURE	Page: 2 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

- e) Ensuring the Security Request Form contains the proper approval;
- f) Ensuring the Security Request Form is routed for appropriate approval, including corporate approval if required;
- g) Ensuring the Security Request Form is routed to the appropriate party for processing;
- h) Ensuring a copy of the Security Request Form is maintained by the entity responsible for establishing the access. Forms shall be maintained until the UserID has been deleted, or longer as required: and
- i) Ensuring timely production and review of security reports to determine if User access assigned reconciles to User access requested for all systems.

B. UserID Assignment Standards


The following standards apply when assigning User access to Tenet information assets:

- a) The login name shall be unique. Each User must have his/her own UserID that is unique from the UserIDs of other Users.
- b) A consistent naming convention should be used when entering user data for a new UserID. Whenever possible, the User's social security number and/or last name, first name and middle initial should be obtained from the Human Resource (HR) Department and listed exactly as reported on the HR file.
- c) The initial password for the account shall not be a standard password given to all new accounts. The new account password shall be unique, and shall not be the same as the UserID.
- d) The new account password shall expire the first time it is used, requiring the User to change the password as part of the initial login procedure.

Refer to UserID Control Procedure No. 8.1.1 for further information.

C. Modification Requests

Modifications to UserID access privileges shall be performed in such a way as to ensure that the modifications are properly authorized.

	Information Security Policies and Procedures	No. COMP-Sec 3.1.1
	Title: ACCESS REQUEST AND MODIFICATION PROCEDURE	Page: 3 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

- a) Requests to change access or privilege levels shall follow the same procedure as the original request.
- b) Individuals who change their names shall have their name changed on their existing user accounts, but may not have the actual UserID changed due to tracking considerations.


D. Special Requests

- a) Generic UserIDs are generally prohibited on production systems. These include application, system, training and test UserIDs. These UserIDs shall not be assigned without approval of the Corporate Privacy/Security Office.
- b) Bulk UserID loads are generally prohibited without documentation. These include any process where multiple users are granted access to a system without following the Security Request Form process (e.g. loading all risk managers into a new risk management system). Bulk UserID loads should not be performed without approval of the Corporate Privacy/Security Office. Documentation of the bulk load should contain the following for each user (see sample attached hereto as Addendum "C"):
 - (i) UserID;
 - (ii) Full name;
 - (iii) Facility, department, and title;
 - (iv) Date UserID will be activated; and
 - (v) Reason why this individual is eligible to receive access during the bulk load.

E. Perot Systems' Security Provisions


Perot Systems has appointed a Security Account Interface to assist facility management and points-of-contact in addressing security issues and concerns. System security requests and questions shall be directed to the Perot Systems Security Account Interface via the Perot Systems Support Line for Tenet at 800.639.7575.

IV. RELATED DOCUMENTS AND REFERENCES

	Information Security Policies and Procedures	No. COMP-Sec 3.1.1
	Title: ACCESS REQUEST AND MODIFICATION PROCEDURE	Page: 4 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- User Security Policy No. 3.0.0.
- Information Access Controls Standard No. 3.1.0.
- Access Termination Procedure No. 3.1.2.
- Technical, Maintenance and Housekeeping Personnel Access and Supervision Procedure No. 3.1.3.
- Security Administration Policy No. 7.0.0.
- Asset Access Controls Standard No. 8.1.0.
- UserID Control Procedure No. 8.1.1.
- Tenet Information Systems Policies and Procedures No. 2.35 “Sensitivity, Confidentiality, and Appropriate Use”.
- Tenet Privacy Policies and Procedures No. 1.2.2 “Minimum Necessary”.

	Information Security Policies and Procedures	No.	3.1.1
	Subject: Access Request and Modification Procedure	Page:	5 of 7
		Original Date:	10/27/00
		Revised Date:	12/14/01
		Approved:	Connie Emery

ADDENDUM A

SECURITY REQUEST FORM FOR CORPORATE MANAGED APPLICATIONS

The form and instructions can be found on eTenet at:

<https://secure.etenet.com/Departments/InformationSystems/Forms/Security/security.htm>

Tenet Healthcare Corporation

Proprietary

ADDENDUM B

SAMPLE HOSPITAL SECURITY REQUEST FORM

Facility Name <i>Security Request Form</i>		
First Name:	Middle Initial:	Last Name:
Phone:	Date:	Last four digits of SSN:
Department:	Title:	
SOFTWARE/ACCESS REQUEST Please check all appropriate boxes	Employee Type: <input type="checkbox"/> Temporary <input type="checkbox"/> Full Time	
<u>APPLICATIONS:</u>		
<input type="checkbox"/> ORSOS	<input type="checkbox"/> Pyxis	<input type="checkbox"/> PowerScribe
<input type="checkbox"/> Cerner	<input type="checkbox"/> Ascend IP	<input type="checkbox"/> SoftMed
<input type="checkbox"/> QuadRIS	<input type="checkbox"/> STAR	<input type="checkbox"/> EPF
<input type="checkbox"/> Other (specify)		
<u>DOMAIN ACCESS</u>	<input type="checkbox"/> ten_hsp_domain	<u>NETWORK DRIVES:</u> <input type="checkbox"/> S <input type="checkbox"/> H
<u>SPECIAL REQUEST:</u>		
<input type="checkbox"/> Word <input type="checkbox"/> View Only	<input type="checkbox"/> Excel <input type="checkbox"/> View Only	<input type="checkbox"/> Outlook
<input type="checkbox"/> Powerpoint	<input type="checkbox"/> Access	<input type="checkbox"/> Wordperfect
<input type="checkbox"/> Lotus 123	<input type="checkbox"/> Other: _____	

For ISD use only	
------------------	--

Notes: _____

I understand that I am being issued a security logon to access the Tenet network. This logon is to be treated with utmost confidentiality and I am the only one who will log on with this code.

_____	_____
User Signature	Date
_____	_____
Supervisor Signature	Date

Computers, computer files, the e-mail system, the voice-mail system, and software furnished to employees are Tenet property intended for business use. Voice-mail system, and e-mail system, numerous computers, including portable computers, computer terminal, software, and numerous Internet-connected terminals are available to assist Tenet in conducting business, internally and externally. These systems, including the equipment and the data stored in the systems and all information and materials downloaded into Tenet computers are and remain the property of Tenet. Employees should not use a password, access a file, or retrieve any stored communication without authorization. To ensure compliance with policy computer and e-mail usage may be monitored.

Tenet Healthcare Corporation

Proprietary

ADDENDUM C

SAMPLE BULK USERID LOAD

UserID	Full Name	Facility	Department	Title	Date UserID Activated	Eligibility for Bulk Load
jdoe123	John Doe	Tenet Service Center	Corporate IS	Director	9/30/04	Part of corporate IS directors group; needs access to perform function.

Tenet Healthcare Corporation

Proprietary