	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 1 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

Access Termination 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

This document provides guidelines for terminating a User’s access to Tenet information assets. When a User’s relationship to Tenet changes, it may be necessary to change the User’s access privileges. These changes shall be accomplished timely when the User’s relationship to Tenet is being terminated. Refer to Human Resources policies and procedures for further information.


Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception will be documented and maintained by the controlling entity in its Information Security Controls Exception Book.

III. PROCEDURE

A. Types of User Status Change

There are five types of User status changes that require termination of access to Tenet information assets:

- a) Voluntary terminations (User’s choice).
- b) Involuntary terminations (Tenet’s choice).
- c) Hostile terminations (Voluntary or involuntary). These terminations may include:
 - (i) Any situation where the individual is being terminated “with cause”.
 - (ii) Any situation where the individual is considered disgruntled.
 - (iii) Any situation where facility management judges the individual would pose a threat to Tenet information assets.

	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 2 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

d) Transfers.

- (i) Transfers involve Users changing departments, jobs, or facilities. The User's access privileges shall be reviewed and approved by the new cost center manager as part of the transfer approval process and as needed new privileges shall be created or existing privileges terminated.


e) Third party user terminations.

- (i) The access privileges for third party Users shall be terminated at the time the User's relationship with the facility is terminated. This applies to contractors, students, physicians, volunteers, and other third parties.

B. Responsibilities

Listed below are the responsibilities to be followed by facility management, the Human Resources Department, and the Information Systems Department for ALL terminations.

Responsible Party	Required Actions
Facility Management	<ul style="list-style-type: none"> • Follow the steps outlined in the Tenet Human Resources policies and procedures. • Review documentation being removed from the premises. • Review electronic media being removed from the premises. If electronic media is not approved for immediate release, an address shall be obtained for later distribution. Encrypted files that cannot be accessed by facility management shall not be released. • Determine who shall become the owner of files (hardcopy and/or electronic) necessary to complete the User's job responsibilities. • Notify the Information Systems Department on or before the date User's relationship to Tenet is terminated.
Human Resources	<ul style="list-style-type: none"> • Follow the steps outlined in the Tenet Human Resources policies and procedures. • Provide an electronic list of terminated employees to the Information Systems Department after every payroll run.


	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 3 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

Responsible Party	Required Actions
Information Systems	<ul style="list-style-type: none"> • Immediately upon notification of User termination disable User's access to ALL information assets including: • Email. • Network. • Locally and Perot administered information assets. • Review the terminated/transferred employee report provided by the Human Resources department to ensure that access for all terminated employees has disabled in the prior two week period.

1. INVOLUNTARY TERMINATIONS

The responsibilities listed below are additional steps that shall be taken to accomplish a termination of access upon an **involuntary termination**.

Responsible Party	Required Actions
Facility Management	<ul style="list-style-type: none"> • Contact the Facility Information Systems Director immediately to ensure that ALL User access has been disabled – this shall be completed before the employee is contacted. • Inform the Facility Security department of the termination. • Ensure the individual is escorted from the premises. • If the User had access to security codes or keys, ensure the codes or key-locks are changed. • Require all immediate coworkers or others who had direct contact with the terminated individual to change their password. • When the terminated individual was responsible for the creation or removal of UserIDs from any system, facility management shall consider implementing immediate password change requirements for all Users on that system.
Human Resources	<ul style="list-style-type: none"> • Follow the steps outlined in the Tenet Human Resources policies and procedures. • Provide an electronic list of terminated employees to the Information Systems Department after every payroll run.

	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 4 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

Responsible Party	Required Actions
Information Systems	<ul style="list-style-type: none"> • Assist facility management in reviewing any electronic media being removed from the premises. • Reset the passwords of all immediate coworkers or others who had direct contact with the terminated individual. • Consider the need to examine the individual's files and activities for evidence of code that could activate after their departure and cause harm to Tenet data or assets.

2. *TRANSFERS*


The responsibilities listed below are steps that shall be taken to accomplish a termination of access upon a **transfer**.

Responsible Party	Required Actions
Facility Management	<ul style="list-style-type: none"> • Determine the expected date of transfer. • Notify Information Systems of the transfer and date.
Information Systems	<ul style="list-style-type: none"> • Determine user access changes that need to be made and disable UserIDs from the appropriate information assets as of the date of transfer.

3. *TERMINATION OF THIRD PARTY ACCESS*

The responsibilities listed below are additional steps that shall be met to accomplish a termination of access upon **termination of third parties**.

Responsible Party	Required Actions
Facility Management	<ul style="list-style-type: none"> • Notify the Information Systems Department when User access requirements change. • Request that Tenet materials such as keys, key cards, identification badges, access tokens and other items be returned. • Periodically, request a terminated/transferred employee file from the contractor to identify individuals who are no longer supporting the contract requirements.
Information Systems	<ul style="list-style-type: none"> • Remove UserIDs from the system immediately upon request from facility management. • Disable UserIDs from the information assets as of the

	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 5 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

Responsible Party	Required Actions
	date of transfer.

4. *USERS WHO HAVE ADVANCED LEVELS OF ACCESS*

Individuals responsible for system administration may warrant special consideration. The individual manager in conjunction with representatives from Human Resources and Information Systems shall determine if special consideration is appropriate. Actions may include:

- a) Placing an audit trail or log on the User's account to track access for several days prior to the termination;
- b) Reviewing the User's previous work activities in an attempt to identify any 'trojan horses' or 'time bombs';
- c) Upon termination, resetting all passwords on the systems administered by the User;
- d) Reviewing all UserIDs and access privileges to ensure that each is assigned to a legitimate User and privileges are at the appropriate level.

5. *CHECK-OUT PROCEDURES*

It is recommended that check-out procedures be used to ensure system access is removed when a user terminates his/her relationship with the facility. Prior to finishing their last shift or receiving their last paycheck, the Users should be required to visit each system administrator and obtain a check-out signature verifying that their access has been disabled.


C. UserID Administration

1. UserIDs Not Accessed in 90 Days

When a UserID has not been used for a period of ninety (90) days, that UserID shall be disabled.

2. UserIDs Not Accessed in 180 Days

When a UserID has not been used for a period of one hundred eighty (180) days, the User's manager shall be contacted and the following steps shall be taken:

	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 6 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

- a) Special consideration shall be granted for UserIDs and data that belong to employees who are on a leave of absence or extended deployment outside of their normal operating environment (and expected to return).
- b) If there are files associated with this UserID and the UserID is to be removed from the system, the User's manager shall determine if the files shall be transferred to another User, archived or deleted.
- c) The UserID shall be removed from the system.


D. Schedule for Retention of Files

Unless the System Administration staff has received instructions to the contrary, four (4) weeks after a User has permanently left Tenet, all files held in that User's directories shall be archived or deleted.

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.
- User Security Policy No. 3.0.0.
- Information Access Controls Standard No. 3.1.0.
- Access Request and Modification Administrative Procedure No. 3.1.1.
- Asset Access Controls Standard No. 8.1.0.
- UserID Control Procedure No. 8.1.1.
- Tenet Administrative Policies and Procedures No. 1.11 "Records Management".
- Tenet Human Resources Policies and Procedures No. 901 "Termination of Employment".

	Information Security Policies and Procedures	No. COMP-Sec 3.1.2
	Title: ACCESS TERMINATION PROCEDURE	Page: 7 of 7
		Revised Date: 12/22/04
		Original Date: 10/27/00

- Tenet Human Resources Policies and Procedures No. 903 “Reductions in Force and Severance Pay”.
- Tenet Human Resources Policies and Procedures No. 904 “Exit Interviews”.