	Information Security Policies and Procedures	No. COMP-Sec 8.1.1
	Title: USERID CONTROL PROCEDURE	Page: 1 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

UserID 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 administration and maintenance of UserIDs. UserIDs are an important component of User access controls at Tenet and demand proper configuration, application and administration.

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. UserID Administration

The creation of new UserIDs shall be the responsibility of system or security Administrators.

- a) Creation of UserIDs for individual use is restricted to the appropriate procedures as outlined in the Access Request and Modification Procedure No. 3.1.1.
- b) For those information assets where the Access Request and Modification Procedure No. 3.1.1 does not apply, the system Administrator shall use those procedures as a guideline to document alternate procedures.
- c) Each UserID shall be unique to each User.
- d) UserIDs shall be administered in such a manner that risks from UserID sharing, impersonation, excessive privileges, etc., are limited.

B. Types of UserIDs

	Information Security Policies and Procedures	No. COMP-Sec 8.1.1
	Title: USERID CONTROL PROCEDURE	Page: 2 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

UserIDs can be interactive (between a User and an asset) or non-interactive (between an asset and an asset). So that their access may be revoked timely on short notice, records reflecting computer systems and applications to which Users have access shall be kept up to date.

1. Standard UserIDs

An individual's UserID that enables access to information assets for performance of Tenet business functions.

- a) Allows interactive access.
- b) Default privileges shall be set to the minimum needed to perform a User's job requirements.
- c) Whenever possible, User logons shall proceed to a menu rather than a command prompt.

2. Generic UserIDs


Interactive generic UserIDs cannot be identified with an individual User and shall not be permitted, with the following exception:

- a) Generic UserIDs are permitted for network/desktop operating system access in shared environments, where:
 - (i) The operating system password does not in itself provide any access to *CONFIDENTIAL* or *PROPRIETARY* information; and
 - (ii) Each User uses his/her own unique UserID to gain access to the systems and applications on that workstation.

3. Application UserIDs

A UserID employed by one information asset to access another asset (often used for batch or other processing).

- a) Interactive access is not allowed.

	Information Security Policies and Procedures	No. COMP-Sec 8.1.1
	Title: USERID CONTROL PROCEDURE	Page: 3 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

b) The UserID shall contain information that relates it to the name of the application (i.e. S2K###).

4. System UserIDs

Can be either interactive or non-interactive and are used by an operating system to run the asset (i.e. server, router).

- a) UserIDs loaded by the vendor, such as root, system, field, etc.; pose a security risk; and:
 - (i) Shall be disabled and/or renamed before being placed into production.
 - (ii) Shall be restricted to their specific job function.
 - (iii) Shall be documented, logged, monitored and audited on a routine basis.

5. Test UserIDs


Interactive or non-interactive UserIDs provided to individuals for testing the functionality of a system or application.

- a) Shall not be assigned to production systems, applications, or databases.
- b) Shall be created, used and deleted based on individual need.
- c) Shall have the minimum access required to test the system, software, or function they are designed to test.
- d) Shall have an expiration period equal to or less than ninety (90) days.
- e) Shall be subject to non-use termination requirements. See the Access Termination Procedure No. 3.1.2 for further information.

6. Training UserIDs

Interactive UserIDs provided to individuals for training on a system or application.

- a) Shall not be assigned to production systems, applications, or databases.

	Information Security Policies and Procedures	No. COMP-Sec 8.1.1
	Title: USERID CONTROL PROCEDURE	Page: 4 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

- b) Shall be created, used and deleted based on individual need.
- c) Shall have the minimum access required to perform the training.
- d) Shall have an expiration period equal to or less than ninety (90) days.
- e) Shall be subject to non-use termination requirements. See the Access Termination Procedure No. 3.1.2 for further information.

7. Privileged UserIDs


UserIDs granted on a restricted basis to those administrators, operators or other system level individuals requiring powerful, interactive access in the performance of their jobs. These UserIDs may have the authority to by-pass security features built into systems, files and applications.

- a) When performing privileged functions, system administrators shall use a unique UserID different from the administrator's own personal UserID.
- b) Shall be logged, monitored and audited on a routine basis.
- c) Shall have an expiration period equal to or less than thirty (30) days.
- d) Any individual with a UserID that has advanced privileges and access shall have a second UserID assigned that has a restricted or "Normal" privilege level.
 - (i) The individual shall use the non-privileged UserID for day-to-day business and the advanced UserID only when needed.

8. Client, Agent Or Customer UserIDs

Interactive or non-interactive UserIDs provided to individuals who are not employees of Tenet, but who require access to Tenet systems to support or perform Tenet business functions.

- a) Allows transfer of or access to data.
- b) Shall provide the minimum access required for the individual and their purpose.

	Information Security Policies and Procedures	No. COMP-Sec 8.1.1
	Title: USERID CONTROL PROCEDURE	Page: 5 of 5
		Revised Date: 12/22/04
		Original Date: 02/16/01

c) Shall be subject to the non-use termination requirements. See the Access Termination Procedure No. 3.1.2 for further information.

C. Privileges For Non-Employee UserIDs

No advanced access unless provided by exception through contractual agreement (i.e. IT administration, vendor service).

D. Concurrent Logons

Networks, systems, and applications should be configured to disallow more than three (3) concurrent logons for a single UserID. If more than three (3) concurrent logons are required, then approval is required from the Corporate Privacy/Security Office.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Information Handling Procedure No. 2.1.1.
- User Security Policy No. 3.0.0 and its subordinate Standards and Procedures.
- Technical Security Management Policy No. 8.0.0.
- Asset Access Controls Standard No. 8.1.0.
- Password Control Procedure No. 8.1.2.
- Logging and Auditing Procedure 8.2.2.
- 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.

End of Document