	Information Security Policies and Procedures	No. COMP-Sec 3.3.2
	Title: PASSWORD USE PROCEDURE	Page: 1 of 6
		Revised Date: 12/3/07; 12/22/04
		Original Date: 10/27/00

Password Use 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

Provide guidelines for Tenet information asset Users regarding the use of passwords to protect Tenet’s information assets. The individual password is one of the most important security features used by Tenet. Responsible use of passwords is vital to maintaining a secure operating environment.

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

Actions taken under a UserID and password are the responsibility of the UserID owner. UserIDs and passwords must not be shared.


A. Password Use

A unique password should be used for each User who gains access to an information asset storing *CONFIDENTIAL* information. If the system does not require the User to set a password, the User should still set a password that complies with this procedure. This applies to bio-medical devices, RIM devices, PDAs, and other information assets that may not require the user to set a password.

B. Password Structure

All user-chosen passwords shall:

- a) Contain at least eight (8) characters.
- b) Contain both alpha and numeric characters (letters and numbers).

	Information Security Policies and Procedures	No. COMP-Sec 3.3.2
	Title: PASSWORD USE PROCEDURE	Page: 2 of 6
		Revised Date: 12/3/07; 12/22/04
		Original Date: 10/27/00

c) Contain at least one lower case and one upper case alphabetic character.


C. Choosing a Password

Unique passwords can be created by following these guidelines:

- a) String several words together (these passwords are also known as "pass phrases"). An Example: IAmFast1.
- b) Transform a regular word according to a specific method, such as changing a letter to a number reflecting its position in the word. An example: Applesauce becomes 1Pplesauce.
- c) Combine punctuation or numbers with a regular word. An example: texas = Tex1_2as.
- d) Create acronyms from words in a song, a poem, or another known sequence of words. For example, the phrase "I Like To Eat Ice Cream in February", becomes: ILTEiCi2 with the use of the number '2' for February.
- e) Combine a number of personal facts like birth dates and favorite colors "09Red14Blue56".

Do not use passwords that would be easy to guess or crack, including:

- a) Passwords that are identical or substantially similar to the UserID to which it is assigned;
- b) Passwords that are identical or substantially similar to passwords used within a twelve (12) month period;
- c) Any part of your name, a spouse's name, or children's names;
- d) Any part of your street address (street, town, house number, zip code) or your home, work, pager or cell phone numbers;
- e) Any of your family's social security numbers or birth dates;

	Information Security Policies and Procedures	No. COMP-Sec 3.3.2
	Title: PASSWORD USE PROCEDURE	Page: 3 of 6
		Revised Date: 12/3/07; 12/22/04
		Original Date: 10/27/00

- f) Single words found in a dictionary, including proper names, geographical locations, common acronyms, and slang (computer programs can be used to search single word or common passwords); and
- g) Common character sequences such as "123456" or same digit or letter such as "AAAA" or "11111".

D. Changing Passwords


The User shall not be required to change passwords if the following criteria are met:

- a) The User is allowed to change password at any time (every ninety (90) days is recommended) or in the event of a breach; and
- b) Corporate applications:
 - a. Must follow standard practices around inactivity and eID and must have one (1) of the following:
 - i. All sites using application are live with Sentillion SSO (would include any Corporate Citrix application using Sentillion); *or*
 - ii. Application is ADAM-aware; *or*
 - iii. Application is able to define resets by facility;
- c) Facility applications:
 - a. Must be live with Corporate Active Directory;
 - b. Must be live with Sentillion SSO on all workstations using a given application.

Passwords that do not meet the above criteria shall be changed at least every ninety (90) days.

E. Recording Passwords

Passwords shall not be displayed or stored in areas accessible to others, including:

	Information Security Policies and Procedures	No. COMP-Sec 3.3.2
	Title: PASSWORD USE PROCEDURE	Page: 4 of 6
		Revised Date: 12/3/07; 12/22/04
		Original Date: 10/27/00

- a) In your Rolodex under “P” (or anywhere else);
- b) On a sticky note on your terminal;
- c) On a sticker on the bottom of your keyboard;
- d) On the back of an employee badge; and
- e) On your hard drive.

If the password is written down, it shall be disguised and retained with personal possessions at all times (i.e. wallet, purse).

F. Password Sharing is Prohibited


Regardless of the circumstance, passwords must never be shared or revealed to anyone other than the authorized User. If passwords are shared, any actions taken under the password shall be the responsibility of the authorized User.

If password security has been compromised, the password shall be changed immediately and proper incident reporting procedures shall be followed. Withholding information related to Information Security breaches or compromises can subject a User to disciplinary action, up to and including termination.

G. Password Use by Information Systems Personnel

Information Systems (IS) often needs access to Users’ passwords in order to perform support/maintenance. In these scenarios, the following process should be followed:

- a) IS informs the user regarding the support/maintenance services that will be provided using the User’s UserID.
- b) IS resets the User’s password and assigns a new unique password.
- c) IS performs the required support/maintenance.
- d) IS resets the User’s password and notifies the User that his/her password has been reset.
- e) User changes his/her password during next logon to the system.

	Information Security Policies and Procedures	No. COMP-Sec 3.3.2
	Title: PASSWORD USE PROCEDURE	Page: 5 of 6
		Revised Date: 12/3/07; 12/22/04
		Original Date: 10/27/00

H. Automating Password Entry

Tenet information asset Users shall never hard-code (incorporate) passwords into software, workstation function keys, or any shortcut procedure. However, single sign-on mechanisms that forward password authentication from one system to another are permitted.

I. Confidential Information and the Use of Different Passwords

Users shall consider employing two passwords to access systems when one or more holds *CONFIDENTIAL* information (e.g. one password for network access and another password for patient accounting system access).

J. Authentication Tokens

Tokens are hardware items used for advanced authentication (beyond simple UserID and password access). Users are responsible for safe handling and storage of all company authentication devices.

- a) Tokens shall not be stored with the information asset that it is used to access.
- b) If a token is lost or stolen, the loss shall be reported immediately to facility management so the device can be disabled.


K. Effectiveness

The effectiveness of this procedure shall be established through annual audit and review.

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.
- Information Access Control Standard No. 3.1.0.
- Information Security Awareness Training Standard No. 3.2.0.

	Information Security Policies and Procedures	No. COMP-Sec 3.3.2
	Title: PASSWORD USE PROCEDURE	Page: 6 of 6
		Revised Date: 12/3/07; 12/22/04
		Original Date: 10/27/00

- User Conduct Standard No. 3.3.0.
- Incident Handling Policy No. 4.0.0.
- Information Asset Open Area Protection Standard No. 5.2.0.
- Asset Access Controls Standard No. 8.1.0.
- Password Control Procedure No. 8.1.2.