	Information Security Policies and Procedures	No. COMP-Sec 8.1.2
	Title: PASSWORD CONTROL PROCEDURE	Page: 1 of 5
		Revised Date: 12/3/07; 03/31/06
		Original Date: 01/15/01

Password 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 the required configuration and administration of passwords. Passwords are an important component of User access controls at Tenet and demand proper configuration and administration to ensure their security.

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

Information asset Administrators shall ensure that passwords used to access networks, systems, applications and databases are configured to support password controls as outlined in Password Control Procedure No. 3.3.2.

A. Administration Of Passwords

Administrators of Tenet information assets are responsible for configuring systems under their control to enforce compliance with Tenet’s Information Security Policies. Proper configuration can include the use of system controls to reject:

- a) Passwords derived from the individual’s UserID.
- b) Passwords having less than eight (8) characters.
- c) Numeric passwords (no alpha or special characters).
- d) Alpha passwords (no numeric or special characters).
- e) Passwords consisting of all the same characters (*****, AAAAA).

	Information Security Policies and Procedures	No. COMP-Sec 8.1.2
	Title: PASSWORD CONTROL PROCEDURE	Page: 2 of 5
		Revised Date: 12/3/07; 03/31/06
		Original Date: 01/15/01

- f) The six (6) passwords previously selected by the User.
- g) Passwords made up of characters that do not change combined with characters that predictably change. (ABCD01 changes to ABCD02, ABCD03, etc.).

B. Password Expiration


Passwords that meet the requirements of the Password Use Procedure 3.2.2 will not expire. However, it is recommended that the User change the password every ninety (90) days.

Passwords that do not meet the criteria of the Password Use Procedure 3.2.2 should expire at least every ninety (90) days, requiring the User to select a new password.

C. Password Security

Within system limitations, the following guidelines shall be implemented:

- a) The number of consecutive attempts to enter an incorrect password shall be limited, with excessive attempts causing the UserID to be disabled until reset by the appropriate authority. The number of unsuccessful password attempts to be entered before the UserID is disabled shall be set appropriately for the system. If a system does not reject passwords that do not meet the minimum requirements noted in section III.A., the UserID shall disable after three (3) unsuccessful attempts to enter a password.
- b) Failed attempts shall be logged.
- c) Passwords shall be encrypted when held in storage or when transmitted over networks. Password storage files shall not be retrievable by unauthorized Users.
- d) The display and printing of passwords shall be masked, suppressed, or otherwise obscured.
- e) Whenever a system has been compromised, or is suspected of being compromised, the immediate change of every password and re-verification of all UserIDs shall be considered.

	Information Security Policies and Procedures	No. COMP-Sec 8.1.2
	Title: PASSWORD CONTROL PROCEDURE	Page: 3 of 5
		Revised Date: 12/3/07; 03/31/06
		Original Date: 01/15/01

- f) All vendor-supplied default passwords shall be changed before any computer or communications system is put into production.
- g) Strong passwords/pass-phrases (i.e. maximum number of characters, mixed characters and numbers) shall be used with all vendor supplied default UserIDs.

D. Incorporation of Passwords


To allow passwords to be changed when needed, passwords shall never be hard-coded (incorporated) into systems or software. This includes:

- a) Program code (compiled or not).
- b) Batch files (except for single sign-on and other solutions that forward the logon credentials from one system to another).
- c) Automatic log-in scripts.
- d) Software macros.
- e) Executable code.
- f) Terminal function keys.
- g) Other locations where unauthorized persons might discover them.

E. Disclosure of Passwords by Security Administrators

Security administrators shall only assign and disclose a password associated with a new UserID.

- a) When possible, a password reset request shall be fulfilled by placing the new password in the individual's private voicemail. This will require the User to access their voicemail (via pin #), to retrieve the password.
- b) If User access is disabled, the ID shall be enabled without resetting the password unless specifically requested.

	Information Security Policies and Procedures	No. COMP-Sec 8.1.2
	Title: PASSWORD CONTROL PROCEDURE	Page: 4 of 5
		Revised Date: 12/3/07; 03/31/06
		Original Date: 01/15/01

F. Responsibilities Concerning Passwords


Administrators receiving requests for password changes shall positively identify the individual requesting the change.

- a) Users requesting password changes shall prove their identity by providing their name, UserID, and other information that can be verified by the system Administrator.
 - (i) If there is reason to suspect deception on the part of the caller, the request shall be refused pending further investigation. The Corporate Privacy/Security Office should be notified in order that they may conduct an investigation.
 - (ii) If the User cannot provide proper identification, THE REQUEST SHALL BE REFUSED.
 - (iii) An abusive, demanding or threatening User is justification to deny a password change request.
- b) The initial passwords shall be valid only for the initial logon session.
 - (i) Each time a password is reset, a unique password shall be provided.
 - (ii) Accounts shall never be created without a password or with a password that matches the UserID.

G. System Generated Passwords

Tenet facilities using system-generated passwords shall follow these guidelines:

- a) If system-generated passwords are used, they shall be:
 - (i) Created using a truly random password generator.
 - (ii) Generated using a combination of frequently changing seed parameters.
- b) Passwords shall only be generated upon request.

	Information Security Policies and Procedures	No. COMP-Sec 8.1.2
	Title: PASSWORD CONTROL PROCEDURE	Page: 5 of 5
		Revised Date: 12/3/07; 03/31/06
		Original Date: 01/15/01

- c) If passwords or Personal Identification Numbers (PINs) are generated by a computer system, all software and files containing formulas, algorithms, and other specifics of the process shall be controlled with stringent security measures.

H. 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 and its subordinate Standards and Procedures.
- Technical Security Management Policy No. 8.0.0.
- Asset Access Controls Standard No. 8.1.0.
- UserID Control Procedure No. 8.1.1.
- Logging and Auditing Procedure No. 8.2.2.
- Network Access Controls Administration Procedure No. 8.3.2.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.