POLICY # 11.16
SUBJECT: COMPUTER PASSWORD POLICY

POLICY:

It is a policy of The Valley Hospital to develop procedures that provide for the security and maintenance of computer passwords.

PURPOSE:

To establish a standard for creating, securing and maintaining computer passwords.

User IDs and passwords are an important aspect of computer security. A poorly chosen or improperly maintained password may result in the compromise of the computer network. As such, all employees, members of the Medical Staff, volunteers, contractors, vendors, and others with access to the network or applications on machines residing on the network are responsible for taking appropriate steps to select and secure their passwords.

The scope of this policy includes all personnel who meet any of the below criteria:

1. Have a computer account on any Hospital system.
2. Have access to the Hospital network, either on site or remotely.

PROCEDURE:

I. GENERAL

A. All network equipment, computer hardware, computer software, databases and other electronic information resources deemed to be confidential in nature by the Hospital must be protected by user authentication through the use of an individual user ID and a well-formed password. The characteristics of a well-formed password are defined in the attached guidelines.

B. All passwords of system-level administrative accounts must be changed on a quarterly basis. All other user-level passwords (user account, email, etc.,) must be changed every six months.

C. Personnel will be held responsible for all activity performed with their user IDs and passwords.
D. All user-level and system-level passwords must conform to the guidelines described herein.

E. All users of Hospital computer systems are required to safeguard the security of Hospital electronic records in accordance with the “Computer System Security Policy” (#14.16).

II. GUIDELINES

A. See attachment for general password construction guidelines and password protection standards.

B. If enabled, screen saver passwords on PCs should engage after three minutes of inactivity.

C. A user’s password should never be revealed to another user. Anyone requesting to do so should be instructed to call the Information Systems department at x2700.

D. If a user account or password is suspected to have been compromised, it should be reported immediately to the Information Systems department at x2700.

III. PASSWORD AUDITING

A. An audit of all passwords will be performed on a periodic (minimum 90 days) or random basis by the Information Systems department. If a password fails the audit process, the Manager will be notified and the user will be required to change it. The application used to audit passwords will shield the actual password values from the Information Systems staff performing the audit, guaranteeing the privacy of the individual’s password.

IV. USE OF PASSWORDS FOR REMOTE ACCESS USERS

A. This policy shall also apply to personnel accessing the Hospital networks remotely from outside of Hospital facilities.

V. ENFORCEMENT

A. Personnel who violate this policy may be subject to appropriate corrective action, including disciplinary measures. Such action may include, but is not limited to, counseling, suspension or discharge.

RESPONSIBILITY: Chief Information Officer
EFFECTIVE: 03-01-03
Reviewed: 03/31/06; 04/03/08
Attachment: Exhibit A - Guidelines and Standards
Reference: Policy #14.16 – Computer System Security