SUNY DOWNSTATE MEDICAL CENTER
UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

No: HIS - 04

Subject: Password Policy

Page 1 **of** 4

Prepared by: Michael J. Burns, M.Ed., MHA
Reviewed by: Bert Robles, CIO

Approved by: Enterprise-wide Information Services Steering Committee

Original Issued date: 01/05
Supersedes date:
Effective date: 01/05

Distribution
☒ **Administrative Manual**
☒ **Department Manual**
☒ **Patient Care Manual**
☒ **AOD Manual**

Issued by: **HIS Department**

I. PURPOSE:

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change.

II POLICY:

All SUNY Downstate Medical Center employees (including contractors and vendors with access to the Medical Center's automated systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

III. DEFINITION(S):

Application Administration Account – any account that is for the administration of an application (e.g., Oracle database administrator, ORSOS database Manager).

IV. RESPONSIBILITIES:

This policy applies to all Departments and Services implementing HIS and departmental subsystems at the University Hospital of Brooklyn.

V. PROCEDURES/GUIDELINES:

General

- All system-level passwords (e.g., root, enable, NT Administrator, Application Administration Accounts, etc.,) must be changed on at least a **quarterly basis**.
- All production system-level passwords must be part of the UHB administered global password management database.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six (6) months. The recommended change interval is every four (3) months.
- User accounts that have system-level privileges granted through group memberships or programs such as “sudo” must have a unique password from all other accounts held by the user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of “public” “private” and “system” and must be different from the passwords used to log interactively. A key hash must be used where available (e.g. SNMPPv2).
- All user-level and system-level passwords must conform to the guidelines described below.
- **Note**: Always sign-off of the PC whenever you have completed your task(s) and/or if you plan to leave your workstation.

Guidelines:

A. General Password Construction Guidelines

Passwords are used for various purposes at SUNY DMC. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have support for one-time token (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight (8) characters.
- The password is word found in a dictionary (English or Foreign).
- The password is a common usage word such as:
  - **A.** Name of family, pet, friends, co-worker, fantasy characters, etc.
  - **B.** Computer terms and names, commands, sites, companies, hardware, software.
  - **C.** The words “SUNY DMC”, “sanjose”, “sanfran” or any derivation.
  - **D.** Word or number patterns like aaabb, qwerty, zyxwvuts, 123321, etc.
  - **E.** Any of the above spelled backwards.
  - **F.** Any of theabove preceded or followed by a digit (e.g. secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z),
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*0-+/~,
- Are at least eight alphanumeric characters long,
- Are not a word in any language, slang, dialect, jargon, etc.,
- Are not based on personal information, names of family, etc., &
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “The May Be One Way To Remember” and the password could be: “TmB1W2r!” or Tmb1W>r~” or some other variation.

Note: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for SUNY DMC accounts as for other non-SUNY DMC access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various SUNY DMC access needs. For example, select one password for the Engineering systems and a separate password for the HIS systems. Also, select a separate password to be used for an Windows account and a UNIX account.

Do not share SUNY DMC passwords with anyone, including administrative assistants or secretaries. A;; passwords are to be treated as sensitive, **Confidential** SUNY DMC information.

Below are lists of "dont's":

- Don't reveal a password over the phone to **ANYONE**.
- Don't reveal a password in an email message.
- Don't reveal a password to the boss.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.

If some demands a password, refer them to this policy or have them call some in the Hospital Information Services department.

Do not use the "Remember Password" feature of applications (e.g. Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on **ANY** computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every **six (6) months** (except system –level passwords which must be changed quarterly). The recommended change interval is every six (6) months.

If any account or password is suspected to have been compromised, report the incident to HIS and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by HIS or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. The application:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.

- Should provide for some of role management, such as that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+, RADIS and/or X.500 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access of the SUNY DMC networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defined a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrases to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks".

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The *?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I. ATTACHMENTS:

II. REFERENCES:

Date Reviewed	Revision Required (Circle One)		Responsible Staff Name and Title
6/01	YES	NO	Michael Burns, Associate Administrator
12/04	(YES)	NO	Michael Burns, Associate Administrator
	YES	NO	
	YES	NO	