# Information Services and Technology
# Password Policy

## I. PURPOSE

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

## II. APPLICABILITY

This policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any UMDNJ facility, has access to the UMDNJ network, or stores any non-public UMDNJ information.

## III. ACCOUNTABILITY

Under the President, the Senior Vice Presidents shall ensure compliance with this policy. The Vice President for Information Systems and Technology (IST), the President/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of system specific procedures, guidelines and standards.

## IV. DEFINITIONS

Application Administration Account - Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

## V. POLICY

### A. General Principles

1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every three months.

3. 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 that user.

4. Passwords must not be inserted into email messages or other forms of electronic communication.

5. 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 in interactively. A keyed hash must be used where available (e.g., SNMPv2).

6. All user-level and system-level passwords must conform to the guidelines described below.

B. Guidelines

1. General Password Construction Guidelines

Passwords are used for various purposes at UMDNJ. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (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:

a. The password contains less than eight characters.

b. The password is a word found in a dictionary (English or foreign).

c. The password is a common usage word such as:

i. Names of family, pets, friends, co-workers, fantasy characters, etc.
ii. Computer terms and names, commands, sites, companies, hardware, software.
iii. The words "UMDNJ", "sanjose", "sanfran" or any derivation.
iv. Birthdays and other personal information such as addresses and phone numbers.
v. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
vi. Any of the above spelled backwards.
vii. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

a. 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, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

b. Are at least eight alphanumeric characters long.

c. Are not a word in any language, slang, dialect, jargon, etc.

d. Are not based on personal information, names of family, etc.

2. Password Protection Standards

a. 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. If for any reason passwords are written down, they must be kept under lock and key. All password encryptions must adhere to encryption methods as defined in IS&T's Acceptable Encryption Policy.

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

c. Do not share UMDNJ passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential UMDNJ information

d. Don't reveal a password over the phone to ANYONE.

e. Don't reveal a password in an email message.

f. Don't reveal a password to the boss.

g. Don't talk about a password in front of others.

h. Don't hint at the format of a password (e.g., "my family name").

i. Don't reveal a password on questionnaires or security forms.

j. Don't share a password with family members.

k. Don't reveal a password to co-workers while on vacation.

l. If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

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

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

o. If an account or password is suspected to have been compromised, report the incident to IS&T Security Services and change all passwords.

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

3. Application Development Standards

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

a. Should support authentication of individual users, not groups.

b. Should not store passwords in clear text or in any easily reversible form.

c. Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

d. Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

3. Use of Passwords and Passphrases for Remote Access Users

Access to the UMDNJ 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 or a VPN tunnel with a strong password.

4. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines 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 passphrase 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.

## VI. NONCOMPLIANCE AND SANCTIONS

Any person found to have violated this policy may be subject to denial or removal of access privileges to the University network; disciplinary action. under applicable University policies and procedures up to and including termination; civil litigation; and/or criminal prosecution under applicable state and federal statutes