National University of Health Sciences
General Policies

Title: **Password Management**		Page **1** of **3**	
Date Adopted: **4/2/12**		Date(s) Revised:	
James Hinterstein		4/2/12	
President		Date	

POLICY STATEMENT

The purpose of this policy is to establish minimum standards for the creation and protection of each person's University password(s). All users accessing National University of Health Sciences (NUHS) Information Technology (IT) resources are bound by the requirements as described in this policy, to create and secure their password(s).

NUHS relies on the use of University provided credentials (User ID and password) to provide access authentication to online IT resources such as email, institutional data, University websites, academic and personal data, cloud computing processes, and other sensitive services. In particular, passwords are the user's 'keys' to gain access to University information and information systems. A compromise of these authentication credentials directly impacts the confidentiality, integrity, and availability of IT systems, and University as well as user information.

Individuals must have a unique identifier and password for each University account.

- All NUHS owned electronic devices that access confidential/restricted University data must have password protection enabled.
- Passwords must be stored in irreversible encryption format whenever possible.
- Passwords must contain at least eight (8) characters in combination as follows:
  - At least one upper case alphabetic character
  - At least one lower case alphabetic character
  - At least one numeric character (1, 2, 3, etc.)
  - At least one punctuation or symbol character (@, $, #, etc.)
- Passwords must be changed at least once every 45 days.
- Administrator user accounts that have system-level privileges granted through group memberships must have unique passwords for all accounts held by that user.
- System administrators must verify the identity of users when assigning or resetting passwords.

- System administrators should enforce "automatic lock out rules" after five unsuccessful login attempts, when possible.
- All vendor supplied default passwords must be changed prior to any application or program's implementation to a production environment.

General Password Construction and Protection Guidelines

Construction Guidelines

Passwords are used for various purposes. Some of the more common uses include: user accounts, Web account, e-mail accounts, screen saver protection, voicemail passwords, and remote access logins. Since very few systems have support for one-time tokens (dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

- Use random, pronounceable syllables to make up words that are easy to remember.
- Use acronyms for unusual phases that you invent (e.g. WCMPE365D for "why change my password every 365 days").
- Do not select a password that is a common usage word such as "National", "NUHS".
- Do not use computer terms, names, commands, sites, or company's software titles.
- Do not use word or number patterns like abcdefg, qazxsw, 12345678.
- Do not use your account name as your password.
- Do not base your password on any items of personal information such as your name, social security number, birthday, pet names, or family member.

Protection Guidelines

Do not use the same password for NUHS accounts as for non-NUHS accounts (i.e. personal ISP accounts, brokerage accounts, benefit accounts, etc.). Remember if one account password is compromised, all accounts may be compromised. Do not share your University password(s) with anyone, including supervisors, secretaries, or co-workers. All passwords are to be treated as sensitive, confidential NUHS information.

Helpful Tips

Don't reveal your password over the phone to anyone, including your computer support personnel. Support personnel should never initiate a call requesting a password.

- Don't talk about your password around others.
- Don't reveal a password on questionnaires.
- Don't share your password with co-workers while on vacation.
- Don't use the "Remember Password" feature on applications (e.g. Netscape Messenger, Outlook, Outlook Express, Eudora, etc.).
- Don't write passwords down or store them anywhere near your computer.
- Don't store passwords in a file on any computer system (including PDA's or similar devices) without using strong encryption.

Enforcement

The Office of Management Information Systems (MIS) has the responsibility to enforce this policy through systematic means and system users. All National University of Health Sciences students and employees are responsible for complying with this policy. Any student, employee or authorized personnel found to be in violation of this policy may be subject to disciplinary action, up to and including expulsion from the University or termination of employment.

If you suspect your account or password has been compromised, report the event to NUHS MIS personnel, and change your password immediately.

If someone demands your password, refer him or her to this document, or have him or her contact your College Dean or Immediate Supervisor.