

UNC School of Medicine Password Policy

OVERVIEW

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of network resources. As such, all users of information systems on the School of Medicine (SOM) network (including contractors and vendors with access to SOM systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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.

SCOPE

The scope of this policy includes all personnel who have access to the SOM network, or are responsible for an account (or any form of access that supports or requires a password) on any system on the SOM network.

POLICY

General

- All passwords (e.g., email, web, desktop computer, etc.) must be changed at least every ninety (90) days.
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must also be changed when change of employment for any system administrators occurs.
- All passwords must be changed after the initial login.
- Password changes should be unique from previous passwords.
- Minimum time between password changes must be at least 24 hours. This is to prevent users from circumventing the password change requirement by repeatedly changing their password until cycling back to their original password.
- To prevent password guessing, logon accounts should be locked out for 30 minutes after six unsuccessful attempts on systems that support this feature.
- Passwords must not be inserted into email messages or other forms of clear text electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.
- Passwords must not normally be shared with others. If a password is divulged to support personnel for troubleshooting user login issues, then the password should be changed as soon as practical.
- Passwords should never be written down or stored on-line in clear text.

General Password Construction Guidelines

Passwords are used for various purposes. 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. Strong passwords should contain the following:

- Passwords should be at least 6 to 8 characters long.
- Always use a combination of upper- and lower-case letters, including numbers and special characters such as '~!@#\$%^&*()-_+{}|\'";:./?.
- Do not base your password on any items of personal information (e.g. PID, Social Security number, street address, birthdays, names of family members, etc.).
- Do not attempt substitutions of numbers or characters that look like the letter they replace (e.g. C@R0L!N@ for CAROLINA); sophisticated password-cracking programs try these combinations as well.
- For stronger passwords, avoid words or combinations of words that could be found in an English or foreign dictionary, such as "Chapel Hill".
- For best passwords, experts recommend acronyms for unusual phrases that you invent. An example would be the password "~2myuT\$!" for "About 2 more years until Tenure \$alary!"
- Do not use a password that is a common usage word such as:
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "UNC", "tarheel", "sanjose", "sanfran" or any derivation.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- 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: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Password Protection Standards

Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information. Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE, including computer support personnel. Support personnel should never initiate a call requesting a password.
- 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
- Don't attempt to guess another user's password
- Don't use the "Remember Password" feature of applications (e.g., Netscape Messenger, Outlook, Outlook Express, Eudora)

Application Development Standards

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

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

Compromised Passwords

If an account or password is suspected to have been compromised, report the incident to the appropriate system administrators and Information Security Officer and change all passwords.

Enforcement

Auditing Passwords

Systems administrators should periodically run a password "cracking" program on encrypted system password files. Users found to have weak passwords should be notified and their accounts should be flagged to require a password change the next time the user logs onto the system. Electronic or hard copy lists of cracked passwords shall be destroyed immediately and not retained for any reason.

Password Resets

To avoid fraudulent access to the system, any user requiring a reset of his or her password must submit the request in person with an acceptable picture ID. For users that are remotely located or are physically unable to appear in person, password resets must be made via a phone call immediately after faxing two (2) forms of photo ID to the systems support personnel.

In smaller departments, systems administrators may determine the identity of users through personal knowledge of the individual, including visual recognition, voice recognition, etc.

Violations

Any employee found to have violated this policy may be subject to actions up to and including loss of access to network resources and disciplinary action.

Approved by the HIPAA Oversight Council (HPOC): February 4, 2003

Revision History: September 19, 2005