3 Passwords

Policy

This policy applies to all Northern Oklahoma College "Users". The term "users" apply to any person in Northern Oklahoma College, third party contractors, guests, temporaries, licensees, as well as those who represent themselves as being connected – in one way or another – to Northern Oklahoma College who uses, possesses or has access to Northern Oklahoma College communication systems.

General

- All user-level passwords (e.g., email, desktop computer, local/domain, etc.) must be changed at least every 90 days.
- All passwords must contain at least six (8) characters.
- Passwords must not be inserted into email messages or other forms of electronic communication without using approved encryption software.
- All user-level and system-level passwords must conform to the guidelines described below.
- All local accounts (to the system) must conform to the guidelines described below.
- All application passwords must be generated randomly if not managed within the password management database. A standard, default password is not to be granted for all users or groups of users.

Guidelines

Some of the more common uses of passwords include: user level accounts, web accounts, email accounts, screen saver protection, and voicemail password. Due to cost constraints, very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once) and everyone should be aware of how to select strong passwords.

Weak passwords have the following characteristics:

- The password contains less than six (8) characters
- The password is a word found in any language (English, non-English, slang, jargon, proper nouns, etc.)
- The password is a common usage word such as:
    - Names of family members, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aabbccdd, qwerty, zyxwvuts, 12344321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
    - Any of the above with some letters substituted (like passw0rd)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain numbers (0-9)
- Contain at least eight characters.
- Is 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.

Passwords should never be shared with anyone for any reason. If an issue or situation arises that requires you to share your password, immediately change it at the first opportunity.

Password Management

Do not share Northern Oklahoma College passwords with anyone, including administrative assistants or secretaries. The Information Technology Support Staff will be the only exception. 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
- Don't reveal a password in an email message
- Don't reveal a password to your 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
- In summation, don't talk about a password at all

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

Do not use the "Remember Password" feature of applications (e.g., Microsoft Internet Explorer, Microsoft Outlook, Mozilla Firefox, Netscape Messenger, etc.).

IT Security may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it. Password cracking and guessing are not to be performed by anyone outside of IT Security or an approved third party auditor.

Account Lockout

After three (3) consecutive failed login attempts within two (2) hours, the account is locked for good.

Application Development Standards

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

Applications:

- Support authentication of individual users, not groups.
- Must be encrypted on the screen.
- Should not cache the password in a cookie or any other local media format on the client system.
- 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.
- Should provide security capabilities for all sensitive data

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action which could include termination of employment.