University of Nebraska at Kearney
Password Policy

Purpose

The purpose of this policy is to provide guidance for the proper use of passwords at the University of Nebraska at Kearney and to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

Scope

This policy applies to all employees, contractors, consultants, temporaries, and students who are responsible for an account or any form of access that supports or requires a password or PIN on any system that resides at any UNK or NU facility, has access to the UNK network, or stores any non-public UNK information. All user-level and system-level password must conform to the guidelines described below.

General Policies

- Do not share or reveal a password to anyone, regardless of the circumstances.
- Do not write down and store passwords near their computers.
- Do not reveal a password in an email message or through other electronic communciations.
- Do not reveal a password on a questionnaire or form.
- Default passwords of applications or systems must be changed immediately after installation.
- Initial passwords or reset passwords must be set to the highest level possible.
- Users are responsible for all activity performed with their user-IDs and passwords.
- User-IDs and passwords may not be utilized by anyone but the individuals to whom they have been issued.
- Users must not allow others to perform any activity with their user-IDs and passwords.
- Users must not perform any activity with user-IDs and passwords belonging to other users.
- Do not use the same password for UNK accounts as for other non-UNK access (e.g. personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various UNK access needs.
- Do not use the "Remember Password" feature of applications.
- If an account or password is suspected to have been compromised, report the incident to the UNK Information Technology Services Helpdesk and change all passwords.

Policy

When technically feasible, this password criteria will be implemented in current computer systems to secure IT resources. As new computer systems are purchased, password capability should meet this password criteria.

- Each system requires that passwords be changed at least every 90 days.

- Each system requires that all passwords have at ten (10) characters.
- Each system checks the length of passwords automatically at the time that users construct or select them.
- After five unsuccessful attempts to enter a password, each system will suspend the involved user-ID until reset by a system administrator.
- The password file maintained by the application should be encrypted.
- At a minimum, the previous ten passwords can not be reused.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

Systems and application administrators will ensure that vendor supplied accounts are secure. Such account should be enabled only when necessary for vendor access. This applies to operating system and application software

General Password Construction Guidelines

Poor, weak passwords have the following characteristics:

- The password contains less than ten characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "UNK", "Kearney", or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patters 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).

Strong passwords have the following characteristics:

- The password contains both upper and lower case characters (e.g. a-z, A-Z)
- The password has digits and punctuation characters as well as letters (e.g. 0-9, 1234567890_+\";:<>,./?)
- The password is at least ten alphanumeric characters long.
- The password is not a word in any language, slang, dialect, jargon, etc.
- The password is 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 "This 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!