Nashville State Community College

NSCC Policy 08-06-00 Password Policy

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.

Definitions

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 Nashville State Community College's entire network. As such, all Nashville State Community College employees (including contractors and vendors with access to Nashville State Community College systems) are responsible for taking the appropriate steps to select and secure their passwords.

The scope of 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 Nashville State Community College facility, has access to the Nashville State Community College network, or stores any non-public Nashville State Community College information.

Policy

1. General Policy

    a) All administrative information system system-level passwords (e.g., root, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
    b) Vendor-supplied defaults including passwords and Simple Network Management Protocol (SNMP) community strings are to be changed before installing a system on the network and unnecessary accounts are to be eliminated.
    c) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.
    d) 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.
    e) Passwords must not be inserted into email messages or other forms of electronic communication.
    f) All user-level and system-level passwords, except for Banner system passwords, must conform to the guidelines described below.

4. General Password Construction Guidelines

Passwords are used for various purposes at Nashville State Community College. Some of the more common uses include: Banner accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since no current 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:

- The password contains less than eight 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 "Nashville State Community College", "NSCC", or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - 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)

Strong passwords have the following characteristics:

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

5. Password Protection

Do not use the same password for Nashville State Community College accounts as for other non-Nashville State Community College access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same

password for various Nashville State Community College access needs. For example, select one password for the Banner systems and a separate password for email systems.

Do not share Nashville State Community College passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Nashville State Community College 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 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

If someone demands a password, refer them to this document or have them call someone in the Technology Services Division Help Desk.

Again, 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.

Change passwords at least once every three months (except system-level passwords which must be changed monthly).

If an account or password is suspected to have been compromised, report the incident to TSD Helpdesk and change all passwords.

6. System-specific policies: Banner ERP System

- Banner users will be prompted to change their password every 90 days.

- There will be a grace period of 10 days during which the user is reminded at login that their password will expire. The password can be changed from the "Change Banner Password" link on the main Banner menu screen, GUAGMNU. If the grace period expires before the password is changed, the user will receive the change password screen at login and must change their password at that point in order to log in to Banner.

- If an incorrect password is entered three times, the account will be locked for one hour.

- A Banner session will be automatically logged out when it has been idle for 45 minutes. This does not affect a session in which a process is running even if there is no keyboard or mouse input and there are no screen changes.

  The Password Verification program will validate Banner passwords as follows:

  - A Banner password cannot be the same as the login name; a random value is used and communicated to the user by telephone (these passwords must be changed upon the first login).

  - New Banner passwords cannot be the same as any of the past three passwords, and must differ by at least three characters.

  - Banner passwords must be at least eight characters in length, and must contain upper and lower case letters, numbers and one of the following: ! # ? % ^ & * + _ =

  - Special characters @ and $ will not be allowed in Banner passwords to avoid potential problems in certain Banner processes.

7. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Change Log

Date	Change	By
7/5/2016	Modified for stronger Banner ERP passwords	PAK
10/26/2017	Modified Banner idle timeout to 45 min. from 20	PAK
3/15/2021	Modified for new policy format	PAK
6/21/2021	Added General Policy 1.b “Vendor supplied defaults”	PAK

Approved by President’s Cabinet 6/14/21