Password Policy

1.0 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 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, as outlined below, to select and secure their passwords.

2.0 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.

3.0 Scope
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.

4.0 Policy
4.1 General
- All administrative information system system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.
- 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.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at Nashville State Community College. Some of the more common uses include: Plus and 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!

B. Password Protection Standards

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 Plus 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 "dont's":

- 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 Information Security Department.

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 CSD Helpdesk and change all passwords.

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