



San Juan College

Office of Technology Services

Operational Policies & Procedures

Password Management Policy

June 4, 2007

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

Note: This policy is written with the understanding that all accounts and related content is the property of San Juan College.

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 San Juan College facility, has access to the San Juan College network, or stores any non-public San Juan College information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the OTS administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) will require change every 180 days. The recommended change interval is every 90 days.
- Passwords must not be inserted into non-encrypted mail messages or other forms of non-encrypted electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.
- Do not use the same password for San Juan College accounts as for other non-San Juan College access (e.g., personal ISP account, option trading, benefits, etc.)
- Do not share San Juan College passwords with anyone, including administrative assistants or work studies. If access to an account is needed for a work-related necessity and the user is not available, please contact the Office of Technology Services for assistance.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at San Juan College. 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.

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 "San Juan College", "sanjuan", "sjc" 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, !@%^&*()_+|~-=`{}[]:~<>?,.).
Note: Do not use \$#/or\ as some SJC systems cannot accept these special characters.
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- 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

All passwords are to be treated as sensitive, Confidential San Juan 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 a non-encrypted email message
- 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

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

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

C. Use of Passwords and Passphrases for Remote Access Users

Access to the San Juan College Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

5.0 Enforcement

If San Juan College security is breached as a result of a violation of this policy, the person guilty of such violation may be subject to disciplinary action, up to and including termination of employment.

6.0 Approvals

Approved by: _____