University of the Southwest Password Policy

Effective 3/29/2006

1.0 Overview

Passwords are an important aspect of the University's information security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the University of the Southwest network. As such, all University of the Southwest employees 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 University of the Southwest, has access to the University of the Southwest network, or stores any non-public University of the Southwest information.

4.0 Policy

4.1 General

1. All system-level passwords (network administration accounts) must be changed on at least a quarterly basis.
2. All user-level passwords (e.g., Windows, CAMS, USW employee computer, USW Portal Login, etc.) must be changed at least every 60 days.
3. All user-level and system-level passwords must conform to the guidelines described below.
4. Technology Services does not maintain a list of passwords. Should a password be forgotten, it will be reset and the user will be required to create a new password at first login.
5. The password policy WILL NOT AFFECT student email accounts, computer lab accounts, or student organization accounts.

4.1 Password Requirements

6. The password is at least eight (8) characters long.
7. The password contains characters from at least three of the following four categories:
    - English uppercase characters (A - Z)
    - English lowercase characters (a - z)
    - Base 10 digits (0 - 9)
    - Non-alphanumeric (For example: !, $, #, or %)
8. The password **may not** contain three or more characters from the user's account name.
9. The password must be unique to the previous four passwords used.

4.1 Password Guidelines

Poor, weak passwords have the following characteristics:

1. The password is a word found in a dictionary (English or foreign)
2. 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 "<Company Name>", "sanjose", "sanfran" 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., secret 1, 1 secret)

Strong passwords have the following characteristics:

1. Contain both upper and lower case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters e.g., 0-9, ! @#$%^&*()_+|~-=\` { } []:";'<>?,./)
3. Are a minimum of eight alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. Passwords should never be stored on the computer or posted in an obvious location in the office. Passwords may be saved on external storage devices such as USB drives, CD's, etc. Passwords should NEVER be posted in full view.
7. 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!

4.2. Password Protection Standards

1. Do not use the same password for University of the Southwest accounts as for other non-University of the Southwest access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various University of the Southwest access needs. For example, select one password for the Windows login and a separate password for CAMS.
2. Do not share University of the Southwest passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential University of the Southwest information.
3. 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 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
- Don’t use the "Remember Password" feature of applications

If someone demands a password, refer them to this document or have them contact Technology Services.

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

5.0 Screensavers

Screensavers will be enforced to activate after 20 minutes of non-activity. Six seconds after the screensavers activate the system will lock. In order to unlock the system, the user must provide his/her password. The screen saver cannot be changed; however, users will have full access to all other display properties.