UC San Diego Minimum Password Standards

Last updated: June 6, 2014

Overview

Passwords are an important aspect of computer security. They often serve as the first line of defense in preventing unauthorized access to campus computers and data.

A poorly chosen password may result in unauthorized access and/or exploitation of UCSD's resources. All users, including contractors and vendors with access to UCSD systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this document is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all employees or affiliates 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 UCSD’s maintained equipment or has access to UCSD’s maintained network.

UC San Diego Active Directory (AD) Account Construction Requirements

The following outlines the **minimum standards** for password construction.

- Be different from the previous three passwords
- Be at least 7 characters long
- Have characters from at least 3 of the following 4 categories:
    - uppercase,
    - lowercase,
    - numbers,
    - symbols

AD Account Password Change & Inactivity Standards

The following outlines the **minimum standards** for password change frequency.

1. Passwords must be changed at least every 365 days.
2. Accounts that have not been used for 180 days may be disabled
3. Accounts that have been disabled for more than 365 days may be deleted

UC San Diego Business Systems Account Construction Requirements

- Be 6 to 8 characters of mixed alphabetic, numeric, @, #, or $.
- Not contain a common word found in a dictionary

Business System Constraint & Inactivity Standards

- Accounts will be disabled after 5 invalid password attempts
- Accounts will be disabled after 90 days of inactivity

Password Best Practices

Password length more secure than complexity. It's better to have a longer password with less complexity (i.e. 15+ characters) than a 7-8 character with lots of complexity.

PassPhrases: Try to create passwords that can be easily remembered. 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 any of these examples as passwords!

Avoid Using Weak Passwords. Weak passwords have the following characteristics:

- The password contains too few 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 "<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., secret1, 1secret)

Password Protection Standards

- Use different passwords for UCSD accounts from other non-UCSD access (e.g., personal ISP account, option trading, benefits, etc.).
- When possible, use different passwords for different UCSD systems. For example, select one password for Active Directory) and use a different password for Single Sign On
- Do not share UCSD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential UCSD information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the UCSD Security Team (security@ucsd.edu).
- Always decline the use of the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, etc.).

If an account or password compromise is suspected, report the incident to the UCSD security team (security@ucsd.edu).