Division of Information Technology

Password Guidelines

Purpose

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

- Because of diverse campus academic calendars, password expiration may be set to operationally best coincide when campus users are predominately on campus. While best practice dictates password expiration occur usually quarterly, campuses are unique and require more flexibility. Users are strongly encouraged to change their passwords every six months.
- All system privileged account (non-service accounts) passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- Service accounts set to never expire must be approved by the respective unit administrator. Service account passwords should be changed a least annually.
- Password history should be set to 24..
- Minimum password length is 8 characters.
- Maximum password length is 14 characters.
- Password must meet complexity requirements.
- Password must contain at least 3 of the following 4 character types:

    - a lower case letter (a b c d ...)
    - an upper case letter (A B C D ...)
    - number (0 1 2 3 4 5 6 7 8 9)
    - a special character (= + * $?) (! , . @)

- 5 invalid logon attempts within 15 minutes
- Account lockout counter is reset after 15 minutes
- Account lockout duration is 15 minutes
- Account lockout threshold is 10 invalid login attempts.
- Prompt user to change password before expiration is 14 days.
- Passwords must not be inserted into email messages or other forms of electronic communication.

General Password Construction Guidelines

Examples of good passwords that can be remembered:

- A pet's name = Skippy!3Z
- A favorite toothpaste = C0lg@t3!
- A favorite movie = Br@ve_heart!
- It is a good idea to use a different password at the campus than you use at other web sites on the Internet. It is also best if it contains NO dictionary words that can be found in ANY multi-national language.

The followings are characteristics of poor, weak passwords:

- The password contains less than 8 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)

Strong passwords have the following characteristics:

- Is not a word in any language, slang, dialect, jargon, etc.
- Is 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!

Password Protection Standards

- Do not use the same password for campus accounts as for non-CSU access (e.g., personal ISP account, option trading, benefits, etc.).

- Where possible, don't use the same password for various CSU access needs. For example, select one password for the p-card system and a separate password for Office Max system.
- Also, select a separate password to be used for an Windows account and a UNIX account.
- Do not share campus passwords with anyone, including administrative assistants or secretaries.
- All passwords are to be treated as sensitive and confidential 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 coworkers
- 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 Office.

- Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Internet Explorer, etc).
- 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 mobile devices similar) without encryption.
- Change passwords at least once every six months
- The recommended change interval is every 90 days.
- If an account or password is suspected to have been compromised, report the incident to Information Security Office and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis by Information Security Office or its delegates.
- If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.

- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should support LDAP or Windows Authentication security retrieval wherever possible.