CALIFORNIA STATE UNIVERSITY
FULLERTON
INFORMATION TECHNOLOGY

Cal State Fullerton Account and Password Guidelines

Purpose

The purpose of this guideline is to establish a standard for account use and creation of strong passwords which adheres to CSU policy and conforms to NIST Level of Assurance 2 requirements.

User Account Usage, Deletion, Suspension or Termination

Accounts assigned to employees are subject to deletion immediately upon termination of employment unless prior arrangements have been made and approved by the former employee's supervisor.

Accounts assigned to students are subject to deletion one hundred eighty days after graduation or withdrawal from the University unless specific arrangements have been made and approved by the Office of Student Affairs.

Assigned accounts may be suspended (i.e., inaccessible to the user) immediately and temporarily under three circumstances:

- Upon recommendation of the appropriate judicial body in writing or email sent to the Vice President of Information Technology or Information Security Officer;

- When Information Technology staff responsible for systems management have credible evidence that continued use of an account constitutes a threat to the integrity, security, or functionality of computing systems, or to protect the University from liability. Every reasonable effort will be made to notify the Vice President of Information Technology as soon as possible of any such suspension.

- When the account is inactive for 180 (one hundred and eighty) days or more.

Assigned accounts may be terminated immediately and permanently upon the recommendation of the appropriate judicial body in writing or email sent to the Vice President of Information Technology. An individual whose assigned account has been permanently terminated may not seek to have a new account assigned to them without approval of the appropriate judicial body.

Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions will require documentation which justifies the need for a shared account; a copy of the documentation will be shared with the Information Security Office.

Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

Password Creation, Maintenance and Configuration

- Based on security best practices and audit requirements the campus password expiration, in the administrative domains, will be based on forced password changes occurring every year in February, May and September respectively. Additionally, the default domain password policy will be set to enforce password changes every 180 days to assure all passwords meet this expiration requirement
- All system-level (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 Information Security Officer.
- Changed passwords are remembered 24 times and cannot be re-used.
- Minimum password length is 12 characters.
- Maximum password length is 20 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 (= + * $?) (! , . @)

- Account lockout duration is 60 minutes.
- Account lockout threshold is 20 invalid login attempts.

- Passwords must not be inserted into email messages or other forms of electronic communication, with the exception of initial One Time Passwords (OTP).
- All user-level and system-level passwords must conform to the guidelines described below.

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 12 characters
- The password is a word found in a dictionary (English or Non-English)
- 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 Cal State Fullerton accounts as for other non-Cal State Fullerton access (e.g., personal Facebook, Twitter, Instagram accounts, option trading, benefits, etc.).

- Where possible, don't use the same password for various Cal State Fullerton access needs. For example, select one password for the p-card system and a separate password for Office Max system.
- Use a separate password to be used for an Windows, Apple or UNIX accounts.
- Do not share Cal State Fullerton passwords with anyone, including administrative assistants or secretaries.
- All account and account passwords are considered by the California State University as Level 1 protected data.

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 your supervisor
- 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, Netscape Messenger).
- 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 or similar devices) without encryption.
- Change passwords at least once every 3 months
- If an account or password is suspected to have been compromised, report the incident to Information Security Office and change all passwords.

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.

NIST 800-63 Token Requirements

This worksheet will compute the assurance level of a memorized secret token for the given password parameters.

Password parameters meet requirements of Assurance Level:	**2**	
		Bits of Entropy
Password Minimum Length	12	24
Dictionary Check	FALSE	0
Password Composition Rules	TRUE	6
Password Total Bits of Entropy		30

Password Lifetime (in days)	120
Number of failed authentication attempts before locking account	20
Duration of account lock (in minutes)	60

Number of Authentication Attempts Available	57600

	Level 1	Level 2
Maximum allowed probability of successful in-band password guessing attack		
1 in X	1024	16384
2^X	-10	-14
Decimal	0.000976563	6.10352E-05
Number of Authentication Attempts Allowed	1048576	65536

Revised September, 2015