

California State University, Fresno
Information Technology Services
Password (Authentication) Policy

1. Introduction

California State University, Fresno relies significantly upon the use of university provided credentials ("User ID" and password) to provide authentication for access to university data and information technology resources.

Other stronger authentication methods include two-factor credentials that utilize a “something you have and something you know” method of authenticating users. The “something you have” is a hardware device such as a token or smart card, and the “something you know” is a personal identification number (PIN) or other identifier.

Authentication is the process of verifying the identity of users.

The risk of compromise of these authentication credentials used by the university community leads to an increased impact on the confidentiality, integrity and availability of university information resources and data.

Therefore, users are required to take appropriate measures, as described in this policy, to create and secure their authentication credentials.

2. Purpose

The purpose of this policy is to establish minimum standards for the protection, complexity (strength) and change interval of password and two-factor credentials used for authentication.

3. Scope

This policy applies to all users who have or are responsible for user and privileged accounts on Information Technology Services (ITS) information resources.

All Information Technology Services (ITS) managed devices must, if possible, have authentication protection enabled.

This policy applies to all information technology resources managed and operated by ITS.

4. Password Credentials

In accordance with the Fresno State’s Acceptable Use Policy, users are accountable for activities performed with their individually assigned credentials (e.g. "User ID" and password).

Password Security

All university assigned credentials that allow individuals access to confidential (category I) or restricted (category II) data must be part of the university's centrally administered account management system (e.g. integrated into LDAP or Active Directory).

Accounts must be locked out after three incorrect passwords in a 5-minute interval for a period of 5 minutes.

For information resources that support password history management, the minimum standard is for two generations of password changes in the password change cycle.

The minimum password age must be 1 day.

Upon turnover of staff (change of personnel, rotation of job duties, etc.), privileged-level passwords or tokens used for two-factor authentication that are affected by such turnover will be changed or revoked within 30 days of the staff turnover.

If extenuating circumstances exist, a risk-based decision will be coordinated between the appropriate manager and the Information Security Office.

If the account credentials of a user or information resource are suspected of having been disclosed or otherwise compromised, the user, resource administrator or the Information Security Office shall immediately take steps to change and protect the authentication credentials.

Password Strength Requirements

User and privileged level passwords shall be constructed in a manner that minimizes the likelihood of password guessing or brute force attacks.

Passwords must have the following characteristics to ensure strength and complexity:

- Are at least six alphanumeric characters in length.
- Consist of at least three of these four categories
 - Lowercase letters
 - Uppercase letters
 - Numbers (0-9)
 - Punctuation or special characters
(!@#\$%^&*()_+|~=\`{}[]:;'<>?.,./)
- Are not words in any language, slang, dialect, jargon, etc.

Password Change Frequency (Age)

Passwords shall be changed periodically to reduce the impact of disclosure on the confidentiality, integrity and availability of information technology resources and data.

All user-level passwords (e.g., email, web, desktop computer, etc.) for users with access to information resources containing unrestricted data must be changed such that the maximum password age is one year (annual changes). The recommended change interval is every semester.

All user-level passwords (e.g., email, web, desktop computer, etc.) for users with access to information resources containing restricted or confidential data must be changed such that the maximum password age is six months (semiannual changes).

All privileged-level access passwords (e.g. root, domain administrator, local admin accounts, etc.) that do not utilize two-factor authentication must be changed such that the maximum password age is ninety days (quarterly).

Passwords may be changed on a more frequent basis depending upon practices and risk to the information managed, processed or stored.

Operational Security Standards For Password Use

All passwords must be treated as confidential information. As such, users are required:

- Not to use the same password for Fresno State accounts as for other non-university access (e.g., personal ISP account, instant messaging, etc.).
- Not to share your user-level passwords with anyone.
 - You are individually responsible for what is done with your account.
- After receipt of your initial password during account creation, not to reveal a password over the phone, in an email, or other method to anyone.
 - Fresno State will never ask you to reveal your password in unsolicited email messages or telephone calls.
- Not to talk about a password in front of others.
- Not to hint at the format of a password.
- Not to reveal a password on questionnaires, security forms or email solicitations.

If someone demands your password, refer him or her to this policy, your manager, or to the Information Security Office.

Password Protections For Network Logins

User-level accounts that have privileged level rights granted through group memberships or programs such as "sudo" must have a different password than the privileged-level accounts.

Information Technology Services prohibits the transmission of your individually assigned credentials (e.g. "User ID" and password) in clear text. Authentication mechanisms shall use encryption (e.g. SSL or TLS) to protect the login session.

Passwords must not be inserted into email messages or other forms of electronic communication without adequate protection (e.g. end-to-end encryption) of the credentials.

5. Two-Factor Authentication Credentials

This level of protection makes use of token technology in addition to a password, for information resources requiring a higher level of protection than a password alone can provide. The user must physically possess the hardware device and know the associated PIN, in addition to knowing the password associated with the account.

Two-factor Authentication PIN Requirements

A PIN used for ITS information resources must be at least four characters long and must be created with the following:

- A PIN must avoid easily guessed sequences such as “1234” or “abcd”.
- If the PIN is numeric, it must not contain information identifying you such as Social Security Number or other information publicly obtainable about you.
- If the PIN is alphanumeric, it must contain both characters and numbers.
- If alphanumeric, a PIN must not contain easily guessed words.
- If alphanumeric, a PIN must not contain your name or parts of your name, or information publicly obtainable about you (e.g., address, phone or office number)
- A changed PIN must be substantially different from the previous PIN.

In addition, two factor authentication devices must be safeguarded and kept with you at all times. If your device has been lost or stolen, report it to the University Police department.

6. Exceptions

ITS information resources that are unable to comply with this authentication policy require an exemption.

7. Responsibility

Managers are responsible for implementation, adherence and feedback regarding this policy

8. Enforcement

Violations of provisions in this policy will be handled through normal University procedures.