Information Technology Services Standards

Password Standards	Standard No	ITS-2008-S	Rev	F
	Owner	IT Security and Compliance		
	Approved by	Edward Ho, Director IT Security and Compliance		
	Issued 6-24-10		Revised 11-18-21 (Interim)	

Table of Contents

1. Purpose

Passwords are an important aspect of computer security and are the first line of protection for a user account. A poorly chosen password or one that is shared, intentionally or unintentionally, may result in the compromise of the confidentiality, integrity, and availability of Cal State LA resources. As such, all employees are responsible for taking appropriate steps to create and secure strong passwords.

This standard provides guidance to all users and system administrators regarding the security and management of passwords. It establishes a standard for creation, protection, and management of strong passwords.

2. Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein.

ID/Control #	Description	Title
8025.0	**Policy**	**Privacy of Personal Information**
8060.0	**Policy**	**Access Control**
8060.S000	Standard	Access Control
8060.S000	Appendix	Access Control – Examples of Password Management Settings

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the Guidelines, Standards and Laws Page.

3. Entities Affected by this Standard

This standard applies to all users (e.g., faculty, staff, students, affiliates, contractors, etc.) 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 Cal State LA, has access to the Cal State LA network, or stores any non-public Cal State LA information.

This standard applies to all system administrators responsible for establishing or enabling system password parameters.

4. Definitions

a) Administrative Information Systems: Any University information system that supports the storage, retrieval and maintenance of information supporting a major administrative function of the University and any associated administrative data that resides on end-users' local desktop or laptop computers and/or department servers. Administrative information systems do not include systems that directly support the teaching and learning and research activities of the University.

b) Decentralized System: Any data system or equipment containing data deemed private or confidential, or which contains mission-critical data, including departmental, divisional, and other ancillary system or equipment that is not managed by central ITS.

c) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared, or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information. Confidential data must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

d) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

e) Level 3 Public Data: This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard. Knowledge of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets. Publicly available data may still be subject to appropriate University review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

A student may exercise the option to consider directory information, which is normally considered public information, as confidential per the Family Educational Rights and Privacy Act (FERPA). Directory information includes the student's name, address, telephone listing, email address, photograph, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, grade level, enrollment status, degrees, honors and awards received, and the most recent educational agency or institution attended by the student. For bargaining unit student employees, directory information also includes: the name of the department employing the student, the student employee's telephone listing within the department, the student employee's email address within the department and the student employee's job classification.

f) Password**:** Any secret string of characters that serves as authentication of a person's identity and that may be used to grant or deny access. Passwords are classified as Level 1 Confidential Data.

g) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

5. Standards

5.1 General

Unless authorized by the Information Security Officer (ISO) of the campus, all users of University information assets must be identified with a unique credential that establishes identity. User credentials must require at least one factor of authentication (e.g., token, password, or biometric devices).

Passwords are a common means of verifying a user’s identity before access is given to an information system or service according to the user’s authorization. Users are responsible for keeping their password confidential and for all transactions made using their passwords.

The following provide the foundation for sound password management:

- Passwords should meet or exceed complexity requirements based on the risk.
- Passwords should be changed frequently based on risk.
- Passwords should be protected from exposure.

With the advancement of technology, passwordless authentication method (e.g., Microsoft Authenticator) is an acceptable alternative to passwords.

5.2 Password Construction

If passwords are poorly chosen, they can easily be guessed either by a person or a program designed to quickly try many possibilities. A good password is one that is not easily guessed but still easy to remember.

Password strength is determined by a password length and its complexity. Users are required to construct their passwords based on the requirements and restrictions indicated below and subject to the constraints of the systems where those passwords reside. The length of a password is more important than the complexity. The longer the password, the better.

5.2.1 Password Requirements

All passwords must conform to the following minimum requirements:

- Minimum of 8 characters (longer is generally better)
- At least one character from each of the following:
  - Upper case letters (A-Z)
  - Lower case letters (a-z)
  - Numeric character (0-9)
  - Non-alphanumeric character (all keyboard characters not defined as letters or numerals). Some University systems may not support non-alphanumeric characters or only support a specific subset.

NOTE to System Administrators

If there are system limitations that do not allow for conformance with the above requirements or there is a need for a higher level of security due to the sensitivity of the data, then the responsible system administrator must specify password requirements and a corresponding password change schedule based on the assessment of risk. Also, there may be instances due to contract or research requirements that necessitate more stringent password requirements.

System administrators should be aware that some password mechanisms have more limited character sets than users would expect (e.g., an application might permit users to enter mixed case passwords but then convert all lower case letters to uppercase before hashing the password) or may accept password characters past the maximum length that is stored or checked.

5.2.2 Password Restrictions

The password should **NOT**:

- Use any names, person, places or things found in a dictionary (English or foreign).
- Increment with every password change (e.g., Password1, Password2, Password3…)
- Have more than two characters repeated consecutively.
- Use adjacent keyboard characters as the entire password (e.g., asdfghjkl, qwertyu, 12345678).
- Use public or personnel information such as family names, social security number, user ID, favorite hobbies, TV shows, movie names, credit card or ATM card numbers, telephone number, birth date, driver's license number, license plate numbers, addresses, anniversary date, or pet names.
- Use words, phrases, or acronyms associated with the University (e.g., "GoldenEagle", etc.) • Use look-alike substitutions of numbers or symbols such as replacing an "I" with a "1."
- Use any of the above spelled backwards.
- Use any of the above followed or preceded by a single digit.
- Be so difficult that it is forgotten if not written down. Think of a phrase such as "This May Be One Way to Remember." Substitute characters, numbers and special characters for the first letter of each word in the phrase. For example: TmB1w2R!.

5.3 Password Protection

After creating a strong password it is imperative to keep it confidential.

All users should **NOT**:

- Enter a password while anyone is watching.
- Write down the user ID and password and then post them on a monitor, telephone or desk, put them under a keyboard or mouse pad, carry them in a wallet or purse, or put them in a PDA device without encryption. If a password must be written down, it should be placed in a secure and private location.
- Use another person's user ID and password.
- Sign on and leave the office without logging off, locking the workstation, or taking other comparable precautions.
- Reveal a password to anyone (e.g., your supervisor, co-worker, family member, etc.) either in person, over the telephone, in an unsecured email message, on questionnaires or security forms.
- Click on a link within an email that asks the recipient to verify a password or other user or account information.
- Hint at the format of a password (e.g., "my family name").
- Use the same password for University business and personal purposes.
- Use the "remember password" feature on websites and other applications.
- Download and execute files from unknown sources.
- Use administrator-level privileges for daily tasks.

5.4 Password Change Schedule

Requiring too frequent password changes often causes users to develop predictable patterns in their passwords or use other means (e.g., writing down and sharing passwords, never logging off, etc.) that will actually decrease the security. In contrast, the higher the maximum password age is set, the more likely the password will be compromised and used by unauthorized parties. The adoption of additional identity authentication methods like Multi-Factor Authentication will reduce the need for password changes. A schedule for the changing of passwords must take into account these conflicting circumstances.

The following schedule will be utilized by system administrators to design and/or enable system parameters for the change of passwords. Failure to comply may result in loss of system access. IT Security reserves the right to extend or disable the access of non-compliant accounts.

Password Conditions	Minimum Frequency of Password Change
Default operating system and application passwords	Change immediately
Passwords that allow or may allow access to Level 1 or Level 2 data (e.g., My*CalStateLA Identity*),	Must be changed every 365 days
Passwords with ability to create application transactions (e.g., create purchase requisitions, approve purchase requisitions, create general ledger transactions)	365 days
First-time passwords (e.g., passwords assigned by IT administrators upon account creation or during password resets)	Must be set to a unique value per user and changed immediately after the first use
For decentralized systems, non-administrative systems or shared resources that do not contain Levels 1 or 2 data and meet the password requirements specified in section 4.2.1	Annually

NOTE to System Administrators

If there are system limitations that do not allow for conformance with the above requirements or there is a need for a higher level of security due to the sensitivity of the data, then the responsible system administrator must specify password requirements and a corresponding password change schedule based on the assessment of risk. Also, there may be instances due to contract or research requirements that necessitate more stringent password requirements.

System users are encouraged to change a password before it expires in order to avoid disruption of access to University services. Email notifications of *MyCalStateLA Identity* password expiration are sent automatically to users 15 and 7 days prior to expiration.

5.5 Password Reuse

Passwords should not be reused. Old passwords may have been compromised or an attacker may have taken a long time to crack encrypted passwords. Reusing an old password could inadvertently give attackers access to the system. *MyCalStateLA Identity* passwords are controlled by system parameters that disallow password reuse until ten different passwords are used.

5.6 Compromised Passwords

Passwords that have been or suspected to have been compromised (e.g., stolen, guessed, etc.) should be changed immediately. Immediately report any incidents when you believe someone else is using your password or otherwise accessing your account to IT Security and Compliance at extension 3-6170.

5.7 Password Management System

Systems for managing passwords should ensure quality passwords. There is always a cost/benefit tradeoff, and the effort placed on the individual should certainly not exceed the value of the assets to be protected.

5.7.1 General

A password management system should:

- Enforce the use of individual user IDs and passwords to maintain accountability.
- Establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password.
- Provide unique temporary passwords to an individual and force an immediate password change.
- Support authentication of individual users, not groups.
- Issue passwords via a secure communication channel (email is not considered a secure communication channel).
- Not display, store or transmit passwords in an unprotected form.
- Maintain a record of previous user passwords and prevent re-use.
- Not display passwords on the screen when being entered.
- Have users acknowledge the receipt of passwords.
- Alert the ID owner if there are several wrong password attempts.
- Have an automated mechanism to ensure that passwords are changed according to the password change schedule.
- Change default passwords to conform to this best practice standard prior to deployment of all software applications, systems and other IT devices on the University network.

5.7.2 Lockout After Failed Login Attempts

After a maximum of nine (9) unsuccessful consecutive login attempts, an account will be locked for 5 minutes after which the user can retry the login routine.

5.7.3 Password Reset

The *MyCalStateLA Identity* account provides an online, self-service offering. Forgotten or compromised passwords can be reset online using the security questions that users create when they activate their *MyCalStateLA Identity* account. Users can remotely reset their passwords from the ITS home page (click on the *MyCalStateLA ID* Quick Links sidebar); or at https://id.calstatela.edu.

IT Security reserves the right to force password reset to contain the risks of user credential compromises and security breaches.

5.7.4 Password Storage

Passwords must be protected when stored. Passwords should:

- Be in temporary storage for only a short time and promptly cleared from temporary storage once they are no longer needed.
- Be in files that are encrypted.
- Have operating system access control features that restrict access to files that contain passwords.

5.7.5 Password Transmission

Passwords may be transmitted over internal and external networks to provide authentication capabilities between hosts. The main threat to transmitted passwords is sniffing, which involves using a wired or wireless sniffer to listen to network transmission. Because of sniffing threats, passwords should not be transmitted across untrusted networks without additional encryption unless the passwords have no value and cannot be used to gain access to any significant resources. Sniffing threats should be mitigated by:

- Encrypting the passwords or the communications containing the passwords.
- Transmitting cryptographic passwords instead of plain text passwords.
- Switching from protocols that do not protect passwords to protocols that do.
- Using network segregation and fully switched networks to protect passwords transmitted on internal networks.
- Replacing a password implementation that exposes the passwords to sniffing with a more secure password-based authentication protocol.

6. Contacts

a. Address questions regarding these standards to: ITSecurity@calstatela.edu.

b. Address questions related to password usage, resets and protection to: ITS Help Desk, Library PW Lobby, 323-343-6170.

c. For questions regarding specific department procedures for decentralized systems, contact the department administrator.

7. Applicable Federal and State Laws and Regulations

Federal	Title
	None applicable
State	**Title**
	None applicable