



Information Technology Services Standards



 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
				Page 1 of 10

Table of Contents

1	Purpose	2
2	Entities Affected by this Standard	2
3	Definitions	2
4	Standards	3
4.1	General	3
4.2	Password Construction	3
4.2.1	Password Requirements	3
4.2.2	Password Restrictions	4
4.3	Password Protection	5
4.4	Password Change Schedule	5
4.5	Password Reuse	6
4.6	Compromised Passwords	6
4.7	Password Management System	7
4.7.1	General	7
4.7.2	Lockout After Failed Login Attempts	7
4.7.3	Password Reset	7
4.7.4	Password Storage	7
4.7.5	Password Transmission	8
5	Contacts	8
6	Applicable Federal and State Laws and Regulations	8
7	Related Documents	8

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
				Page 2 of 10

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 CSULA 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 Entities Affected by this Standard

This standard applies to all employees 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 CSULA, has access to the CSULA network, or stores any non-public CSULA information.

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

3 Definitions

- a) Level 1 Confidential Data: Confidential information 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. Confidential information is information whose 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 information 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 information to persons outside of the University is governed by specific standards and controls designed to protect the information.
- b) Level 2 Internal Use Data: Internal use information is information which 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.
- c) 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

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
Page 3 of 10				

subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

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

4 Standards

4.1 General

Unless otherwise authorized, all users of campus 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.

4.2 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 passwords 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.

4.2.1 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.

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
				Page 4 of 10

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.

The following are the maximum and approximate amounts of time required for a computer or a group of computers to guess an 8 character password using a brute force “key-search” attack.

Using 8 Characters	Class of Attack (passwords processed per second)					
	A (10,000) Pentium 100	B (100,000)	C (1,000,000)	D (10,000,000)	E (100,000,000)	F (1,000,000,000) supercomputer
Mixed upper and lower case plus numbers and common symbols (96 characters)	22,875 years	2,287 years	229 years	23 years	2-1/4 years	83-1/2 days
Source: LockDown.co.uk – The Home Computer Security Centre. Copyright © 1996-2009. Ivan N Lucas. (March 3, 2009)						

4.2.2 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.

	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
Page 5 of 10				

- 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 “l” 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!.

4.3 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 e-mail message, on questionnaires or security forms.
- 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 Web sites and other applications.
- Download and execute files from unknown sources.
- Use administrator-level privileges for daily tasks.

4.4 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. 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:

Password Conditions	Minimum Frequency of Password Change
Default operating system and application passwords	Change immediately
Passwords with administrative access to	Must be changed every 90 days

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
Page 6 of 10				

Password Conditions	Minimum Frequency of Password Change
Level 1 or Level 2 Data	
Passwords with ability to create application transactions (e.g., create purchase requisitions, approve purchase requisitions, create general ledger transactions)	180 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 systems that 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.

The NIS e-mail system does not currently support password expiration. This condition will be remedied when all existing e-mail systems are merged into a single Identity Manager account, currently in progress.


System users are encouraged to change a password before it expires in order to avoid disruption of access to University services.

4.5 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.

4.6 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 3-2600.

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
Page 7 of 10				

4.7 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.

4.7.1 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 (e-mail 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.

4.7.2 Lockout After Failed Login Attempts

After a maximum of five (5) unsuccessful consecutive login attempts, an account will be locked for 30 minutes after which the user can retry the login routine. If the login routine fails again, the user must request a password reset (see section 4.7.3 below).


4.7.3 Password Reset

Validation of the identity of the user is required prior to performing a password reset on the user's account. Therefore, the user must appear in person with his or her Golden Eagle Card (for employees) or photo identification (for third parties and others) at the ITS Help Desk (LIB PW Lobby).

4.7.4 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.

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
Page 8 of 10				

4.7.5 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.

5 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, contact the department administrator.

6 Applicable Federal and State Laws and Regulations

Federal	Title
	None applicable
State	Title
	None applicable

7 Related Documents


ID/Control #	Title
ITS-1000-G	User Guidelines for E-mail Communications http://www.calstatela.edu/its/policies/ These guidelines are intended to help students, faculty, and staff maintain the University's accepted standard of e-mail use.

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
Page 9 of 10				

ITS-1006-G	<p>User Guidelines for Securing Offices, Workspaces, and Documents</p> <p>http://www.calstatela.edu/its/policies/</p> <p>These guidelines are intended to help the campus community protect offices, machines, devices, and documents from unauthorized access to confidential, personal, and proprietary information.</p>
ITS-1007-G	<p>User Guidelines for Laptop Security</p> <p>http://www.calstatela.edu/its/policies/</p> <p>This procedure outlines the steps for securing laptops and the personal, confidential, and/or proprietary information contained on them.</p>
ITS-1009-G	<p>User Guidelines for Separated Employees' Network/E-mail Access</p> <p>http://www.calstatela.edu/its/policies/</p> <p>These guidelines provide detailed explanations, the procedures and limitations, and the required approvals of network/e-mail access for separated employees.</p>
ITS-1012-G	<p>User Guidelines for Oracle Access</p> <p>http://www.calstatela.edu/its/policies/</p> <p>These guidelines help users understand the different types of Oracle accounts, the process for obtaining one, and compliance requirements for such an account.</p>
ITS-1014-G	<p>User Guidelines for Student Administrative Access</p> <p>http://www.calstatela.edu/its/policies/ITS-1014-G_SAAccountAccess.pdf</p> <p>These guidelines define the criteria for authorized SA access and outline the required steps to obtain and maintain a Student Administration account.</p>
ITS-1015-G	<p>User Guidelines for Wireless Access</p> <p>http://www.calstatela.edu/its/policies/</p> <p>These guidelines help users meet the University's accepted standards for wireless access.</p>
ITS-5002-S	<p>ITS Standards for Creating CMS/PeopleSoft User IDs and Passwords</p> <p>http://www.calstatela.edu/its/policies/</p> <p>This standard defines the characteristics of user IDs and passwords assigned to the CMS/PeopleSoft systems.</p>
NA	<p>Create Strong Passwords</p> <p>http://www.calstatela.edu/its/itsecurity/tips/passwords.htm</p> <p>This Web site provides password dos, don'ts, and tips.</p>
NA	<p>Changing Your Password</p> <p>http://www.calstatela.edu/its/docs/pdf/passwd.pdf</p> <p>This is a handout intended to assist students who have already received their NIS account information.</p>



Information Technology Services Standards

 Password Standards	Standard No:	ITS-2008-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director, IT Security and Compliance		
	Issued:	6-24-10	Effective:	6-24-10
Page 10 of 10				

NA	ITS News (Fall 2004) http://www.calstatela.edu/its/news/fall2004/strongpwd.htm “Open Sesame: The Case for Strong Passwords”
NA	Network/E-mail Account http://www.calstatela.edu/its/helpdesk/nis_account.php Frequently Asked Questions
CSU Information Security Policy	The California State University System-wide Information Security Policy http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.
NA	Password Recovery Speeds http://www.lockdown.co.uk/?pg=combi This document shows the approximate amount of time required for a computer or a cluster of computers to guess various passwords.
NA	Guide to Enterprise Password Management (Draft) http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf Password recommendations of the National Institute of Standards and Technology (NIST)