Creating CMS/PeopleSoft User IDs and Passwords	Document No.	ITS-5002-S	Rev:	--
	Owner:	CMS and Enterprise Systems		
	Approved by:	Bill Chang, Director CMS and Enterprise Systems		
	Issued:	6-24-10	Effective:	6-24-10
				Page 1 of 5

Table of Contents

1 Purpose

These standards define the characteristics of user IDs and passwords assigned to CMS/PeopleSoft accounts in the Human Resources, Student Administration, Contributor Relations, and Finance systems, and are intended to ensure that standard rules are observed when creating user IDs and passwords for these accounts. Properly constructed passwords also guarantee the security and confidentiality of protected data within the CMS/PeopleSoft systems.

2 Entities Affected by this Standard

These standards apply to staff who are responsible for creating CMS/PeopleSoft accounts and all users of those accounts. This document does not apply to students whose accounts are created through a different process and naming convention.

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. 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.

d. 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 User ID Standards

a) Whenever possible, a user should be given the same user ID as their network account ID if it: 1) meets these standards, and 2) is “available” (i.e., not being used by another CMS/PeopleSoft account user).

b) User IDs must contain a **minimum** of three and a **maximum** of eight **UPPERCASE alphanumeric** characters.

c) User IDs must be created in the following format: first initial of the first name plus the first seven characters of last name (e.g., *FLASTNAM*).

d) If the same user ID already exists, then truncate the last name by one character and replace it with the next available numeric character between 1 and 9. For example: *FLASTNA1*. If numeric characters 1 through 9 are already in use, truncate the last name by two characters and replace it with the next available numeric character between 10 and 99. If the last name is less than seven characters, there is no need to truncate the last name before adding the numeric character.

4.2 Password Standards for CMS/PeopleSoft Systems and Portal

a) Passwords must contain a **minimum** of eight characters.

b) Passwords must be **randomly** generated containing a mixture of:
- Uppercase alphabetic characters (A-Z) and
- Numbers (0-9)

c) Passwords cannot contain any of the following:
- User’s names (first, middle, last)
- Dictionary words or words spelled backwards
- Any portion of the user ID
- Public or personal information related to the user (e.g., favorite hobbies, TV shows, movie names, birth date)
- Adjacent keyboard characters as the entire password (e.g., asdfghjkl, qwertyui, 12345678)
- Words, phrases, or acronyms associated with the University (e.g., GoldenEagle, CSULA)
- Any of the above followed or preceded by a single digit.

d) Every password must be unique and any single password cannot be distributed to multiple users. A single password with incremental numbers is not allowed (e.g., password1, password2, password3).

e) Users must be prompted to change their password during the initial login.

f) Passwords can be re-used only after the tenth password reset cycle.

NOTE

Users can find password standards online at:
http://www.calstatela.edu/its/itsecurity/guidelines/ITS-2008-S_ITSPasswordStandards.pdf
http://www.calstatela.edu/its/itsecurity/resources/passwords.php.

4.3 Password Controls Settings

a) Password Aging: 90 days.

b) Account Lockout: Accounts must be locked after three consecutive logon attempt failures.

NOTE

Accounts are locked out permanently after three failures to logon. Gaining access to accounts after lockout requires a password reset by authorized ITS personnel. Users must initiate a password reset request at: http://www.calstatela.edu/its/forms/pwreset.htm.

c) Miscellaneous: Passwords are not allowed to match the user ID.

d) Minimum Length: Eight characters.

e) Character Requirements: The required number of special characters is zero. The required number of numeric characters is one.

NOTE

While information security best practices recommend use of a special character, the current CMS/PeopleSoft environment does not allow for special characters. Should this restriction change in the future, one special character will be required at that time.

5 Contacts

For questions regarding this standard, contact the Director, CMS and Enterprise Systems at 323-343-2654.

6 Applicable Federal and State Laws and Regulations

Federal	Title
	None
State	**Title**
	None

7 Related Documents

ID/Control #	Title
ITS-2008-S	**ITS Password Standards** http://www.calstatela.edu/its/itsecurity/guidelines This document provides best practices regarding the creation, use, and security of passwords.
NA	**Create Strong Passwords – Are you Secure? Tips** http://www.calstatela.edu/its/itsecurity/resources/passwords.php This Web site highlights password dos, don’ts, and tips for creating strong passwords.