



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Password Standard	
Department: Information Security Management and Compliance	Reference No.:
Division: Administration and Finance	Issue Date: February 2008
References:	Revision Date: N/A
Web Links: • http://daf.csulb.edu/offices/vp/information_security	Expiration Date: N/A

I. BACKGROUND

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. Passwords can preserve the confidentiality of password-protected data and are the sole property of account holders. As such, all California State University, Long Beach (CSULB) employees, including contractors and vendors with access to CSULB systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

II. PURPOSE

The purpose of this standard is to communicate the composition of strong passwords, the protection of those passwords, and the frequency of change.

III. SCOPE

This standard applies to all individuals who have or are responsible for an account or any form of access that supports or requires a password on any CSU system, has access to the CSULB network, or stores any non-public CSULB information.

IV. STANDARD

A. Password Composition

Passwords are used for various purposes at CSULB. Some of the more common uses include: user level accounts, email accounts, screen saver protection, voicemail password, and local router logins. To the extent that the password complexity is supported by the respective device, passwords shall:

- Contain at least eight (8) characters
- Contain characters from each of the following four groups:
 - Uppercase letters
 - Lowercase letters
 - Numerals
 - Symbols (all keyboard characters not defined as letters or numerals)
- Not contain personal information such as user name or CSULB ID number of the letters CSULB
- Not contain a complete dictionary word from English or Foreign Language
- Be significantly different from previous passwords
- Not be incremental with every password change (Example: Password 1, Password 2, Password 3. . .)
- Be difficult to crack, but easy to remember (Example: make up a sentence, and then use the first letter of each word or sound, adding a couple of digits or symbols and uppercase letters. For instance, "Tennis anyone??" becomes the password: "10Sne1??" or "I love 8 hot fudge sundaes best," becomes "iL8htfsB!")
- Not have more than two characters repeated consecutively
- Not use adjacent keyboard characters (Example: asdfghjkl, qwertyu, 12345678)

B. Password Protection

Your password is to be treated as confidential information. To protect your confidential information, you should take the following measures:

- Do not use the same password for CSULB accounts as for your personal accounts
- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not talk about your password in front of others
- Do not hint at the format of your password (e.g., "my dogs name")
- Do not reveal a password on questionnaires or forms
- Do not reveal a password to co-workers while on vacation
- Do not write passwords down and store them anywhere in your office
- Do not store passwords in a file on ANY computer systems without encryption
- Do not use the "Remember Password" feature of applications or web browsers

C. Password Change Frequency

The recommended change interval for passwords is every six (6) month.

FURTHER INFORMATION

Information Security Management and Compliance

iso@csulb.edu.

(562) 985-2283