Password Standard

- Issue Date: **February 2008**
- Revision Date: **July 2015**
- Expiration Date: **N/A**
- References:
    - ICSUAM 8060.0 Information Security Policy;
    - ICSUAM 8060.S01 Access Control
- Web Links: Information Security Management and Compliance

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) BeachID accounts, 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. Password Standard applies to all applications that access level 1 and/or level 2 data. This applies to all CSULB, Auxiliary organizations, and third party vendor products used for University business.

Purpose

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

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.

Standard

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, and local router logins.
Passwords shall at least adhere to the following complexity guidelines:

- Be case sensitive
- Be at least ten characters in length
- Contain three of the following four character types:
    - Uppercase English characters (A through Z)
    - Lowercase English characters (a through z)
    - Numbers (0 through 9)
    - Special characters (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /)
- Contain no spaces
- Include no part of a person's full name
- Contain no non-English language characters
- Not match any of a person's previous passwords

To the extent that password complexity is supported by respective devices and/or systems, passwords should also:

- Not contain personal information such as user name or CSULB ID number
- Not contain a complete dictionary word from English or another 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)

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.

National Institute of Standards and Technology (NIST) Criteria

The Password Standard at CSULB for all applications that access level 1 and/or level 2 data are NIST level 2 compliant. In addition to composition rules defined above, the following criteria illustrate the NIST level 2 threshold settings.

NIST Criteria	**Criteria Composition**
Measure	**All User Accounts**
Password Minimum Length	10
Password Lifetime (in days)	365
Dictionary Check	FALSE
Password Composition Rules	TRUE
Number of Failed Authentications before Acct Lock	5
Account Lock Duration (in minutes)	330
NIST Password Threshold Level	**2**

figure 1: NIST Password Standard

Password Change Frequency

System	**Employees**	**Students**
Common Financial System	annual	n/a
Oracle HCM (HR/SA) administrative system	annual	n/a
BeachID/campus LDAP, AD-based systems	annual	annual

figure 2: Password Change Frequency