# CALIFORNIA STATE UNIVERSITY, LONG BEACH

| | |
|---|---|
| Subject: **Windows System Passwords** | |
| Department: **Information Security / Safety & Risk Management** | Reference No.: |
| Division: **Administration & Finance** | Issue Date: **June 2005** |
| References: **Information Security Bulletin (ISB) 2005-01** | Revision Date: **NA** |
| Web Links: **CSULB Information Security** | Expiration Date: **NA** |

An Achilles heel of most Microsoft Windows environments is the weakness of user and administrative passwords. Most Windows systems are compromised because they have at least one account that has a weak password (i.e., easily uncovered by dictionary attack). Even a single weak password is sufficient to provide unauthorized access and thereby compromise the system.

To protect Windows systems from being compromised because of weak passwords, it is strongly recommended that passwords exhibit the following characteristics:

- Contain at least 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)
- Do not contain user name (userid), real name, CSULB, pet name, family's name, favorite hobbies, TV shows, or movie names
- Do not contain a complete dictionary word from English or Foreign Language
- Are significantly different from previous passwords
- Do not increment with every password change (e.g., Password 1, Password 2, Password 3…)
- Are hard 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 digits or symbols and uppercase letters. E.g., "Tennis anyone??" becomes the password: "10Sne1?? Or "I love 8 hot fudge sundaes best, "becomes "iL8htfsB!"
- Do not have more than two characters repeated consecutively
- Do not use adjacent keyboard characters as your password (e.g., asdfghjkl, qwertyu, 1245678).

- Passwords should be changed every 3 months.
- Do not write down passwords, post them on monitors or desks, or attach them under a keyboard or mouse pad.
- Do not share user IDs and passwords with others.
- Enter user ID and password when it is certain that no one is observing.

**FORMS:** NA