California State University Northridge	**Information Technology** CSUN Password Standards and Guidelines	**Page** 1 of 5	
		SOP#: 500-07	**Revision#:**

Prepared by: Unknown **Date:** June 7, 2009	**Approved by:** Previously approved by President as policy 500-07 **Date:** June 7, 2009
Last revised by: Chris Olsen, ISO **Date:** March 11, 2014	**Last approved by:** Chris Olsen, ISO **Date:** March 11, 2014

1.0 STATEMENT

Passwords are an important aspect of CSUN's computer and data security. A poorly chosen password may result in unauthorized access and/or exploitation of CSUN's resources. All users, including faculty, staff, students, guests, contractors and vendors with access to CSUN's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 PURPOSE

The purpose of this standard is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 SCOPE

The scope of this standard includes all users 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 CSUN, has access to the CSUN network, or stores any non-public CSUN information.

4.0 DEFINITIONS

User Account

- General-access account granted to faculty, staff, and students to access university email, campus desktops, the myNorthridge Portal, and other university resources.

System (Administrator) Account

- Granted to system administrators (e.g. "root" or Domain Administrator accounts), and application or database administrators to manage, support, and administer protected university resources such as the campus network, myNorthridge Portal, Identity Management systems, and enterprise Web and Email environments.

Service Account

- Account used by university equipment, services, and applications to access and integrate with other university systems.

Confidential Data User

- User that is granted access to confidential university data such as Social Security Numbers (SSNs), Health Records, and Credit Card information.

5.0 STANDARDS

Length

- Passwords must contain a minimum of eight characters and a maximum of thirty-two characters.

Characters

- At least one upper or lower-case alpha character (a...z, and A...Z);
- At least one numeric character (0...9);
- At least one punctuation or special character (e.g. !, $, &, >, etc.).

Exclusions

- Passwords must not contain your name (first or last), your CSUN UserId, or the word "password."

Expiration, Notification, and Re-Use

- Expiration
    - User account passwords issued to students, faculty, staff, contractors, guests and vendors must be reset at least once every 365-calendar days.
    - System (Administrator) account passwords must be reset at least once every 90-calendar days.
    - Service account passwords must be reset at least once every 365-calendar days.
    - Users with access to university confidential data must reset their passwords at least once every 90-calendar days.

- Notification
    - Users will receive notice of password-expiration to their CSUN email address 3 weeks prior to expiration, weekly thereafter, and the day prior to expiration. During the 3 weeks prior to password-expiration, users will receive notice of expiration upon accessing the myNorthridge Portal and logging into a managed campus desktop computer.
    - Users will receive email notification following each successful password-reset.

- Password Re-Use
    - Passwords can be re-used following six password-resets. A user may reset their password up to two times per 24-hour period.

- Access Prevention - Excessive Bad Password Use
    - User accounts will be "locked" and prevented from accessing university resources for a period of 15 minutes following 50 bad password attempts in a 5-minute period.
    - System (administrator) accounts will be locked for a period of 2 hours following 10 bad password attempts in a 5-minute period.

6.0 GUIDELINES

- Never share your password with anyone; including co-workers, administrative staff, campus technical support staff/administrators (including the IT Help Center), friends and family.
- Do not write down (e.g. post-it notes, etc.) or store your password electronically (unless in an encrypted container).
- Do not create a password containing personally identifiable information. For example; names of friends or family (or pets), birthdays, social security numbers, campus ID numbers, bank account numbers, words or number patterns such as aaabbb or 112233, etc.
- Select a password that is easy to remember and hard for others to guess. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, a phrase might be "This May Be One Way To Remember" and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Do not use the same university password to access other sensitive resources such as bank accounts or other financial resources.

- Systems that interface with, or store confidential data should employ two-factor authentication, where feasible.

Application Developer Password Guidelines

Application developers must ensure their programs contain the following security precautions.

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Shall support integration with campus Identity Management Systems wherever possible.

7.0 APPLICABILITY AND AREAS OF RESPONSIBILITY

VP for IT and Chief Information Officer (CIO)

- The Chief Information Officer (CIO) and all delegated individuals are responsible for the confidentiality of all passwords.
- The CIO is responsible for mandated password changes in an appropriate and timely manner as necessary for maintaining password confidentiality.

Information Security Officer (ISO)

- The Information Security Officer (ISO) is responsible for ensuring that the minimum standards for lifetime, length, and composition of passwords are sufficient to meet prevailing hardware, software, and industry standards for data integrity and for ensuring that these standards meet the needs of the campus to protect the confidentiality, availability, and integrity of protected data and technology resources.

Users and Administrators

- Users are responsible to maintain and update their passwords to preserve the confidentiality of password-protected data. Passwords are the sole property of account holders, and they are required to make a good faith effort to preserve the privacy of their passwords.

8.0 RESOURCES AND REFERENCE MATERIALS

500-02 Desktop Security Lockout

500-8060 Access Control

Application Development Standard

PCI Standard