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: Kevin Krzewinski, ISO **Date:** January 31, 2023	**Last approved by:** Kevin Krzewinski, ISO **Date:** February 1, 2023

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. This also includes all service accounts.

4.0 DEFINITIONS

User Account - General-access account granted to faculty, staff, and students to access university email, campus desktops, the CSUN 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, CSUN 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 as defined in the CSUN Data Classification (https://www.csun.edu/it/protected-data)

5.0 STANDARDS

Length

- User Passwords must contain a minimum of 12 characters and a maximum of 64 characters.
- Administrative and Service Account Passwords must contain a minimum of 32 characters and a maximum of 64 characters.

Characters

A password may contain any characters including spaces and emoji.

Exclusions

- Passwords must not contain your name (first or last), your CSUN User ID, or the word "password."
- Passwords may not equal any single word in the dictionary.
- Passwords may not equal any password from known breach databases.
- Password may not contain repeating letters or numbers greater than three characters.

Expiration, Notification, and Re-Use Expiration

- Regular user accounts will require a password change every two years or more frequently if there is evidence of compromise.
- Once reset, the passwords may not be reused.
- All existing service account passwords will be reset once this policy is implemented.

Third Party Password Requirements

Third party applications SaaS application with multi-factor authentication enabled may use the following password complexity

- Eight characters minimum
- A combination of capital letters, special characters and numbers

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 PASSWORD 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. Do not use your favorite song, pet, spouse, children name or anything on social media.
- Do not use the same university password to access other sensitive resources such as bank accounts or other financial resources.

7.0 MULTI-FACTOR AUTHENTICATION

- Multi-factor authentication is required for all active faculty, staff and students.
- MFA is required to RDP (Remote Desktop Protocol) or SSH (Secure Shell Protocol) to any device (Workstation, Server, etc).
- MFA is required to access any server
- MFA is required on any endpoint device that connects to a database.
- MFA is required to access all CSUN Level 1 data including SaaS applications

8.0 APPLICATION DEVELOPER PASSWORD GUIDELINES

- Applications must support authentication of individual users, not groups.
- Must not store passwords in clear text or in any easily reversible form.
- Shall provide role-based access methods.
- Shall support integration with campus authentication.
- Must use proper key management rotated every 90 days.

9.0 SYSTEM ADMINISTRATION PASSWORD GUIDELINES

- Must use campus authentication.
- Root passwords must never be used and locked in a hardware or electronic cage.
- Must not store passwords in clear text or in any easily reversible form.
- Keys are acceptable passwords. Keys must be rotated every 90 days.

10.0APPLICABILITY AND AREAS OF RESPONSIBILITY

Vice President 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 ISO 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.

11.0 RESOURCES AND REFERENCE MATERIALS

500-02 Desktop Security Lockout

500-8060 Access Control

Application Development PCI

Standard

NIST 800-63

12.0 CHANGE LOG

Date	Author	Change
2/1/2023	Kevin Krzewinski	Added third party section