

# SJSU Password Standard

---

## Executive Summary

---

Passwords are the first line of defense for the computers, communications systems, and information security at SJSU. It is the individuals' responsibility to maintain the security of their password while maintaining a certain level of complexity within that password as not to allow for breeches of that account. Usernames and password management is a significant part of our overall solution to improve security within SJSU. The overall protection of the data assets must begin with the individual who has access to them. Password Standard defines the password requirements surrounding the management of access to information on SJSU's computer and communication systems. The purpose of this standard is to define security protection controls that will help minimize the loss of confidentiality, integrity, and availability of SJSU business information as it is stored, processed, and transmitted.

## Information Security Standards

### SJSU Password Standard

Standard #	IS-AC	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	4.0	Contact	Mike Cook	Phone	408-924-1705

#### Policy History

Date	Action
4/30/2013	Updated/Posted – Standard appended to allow 16-28 character passwords by ISO – Original Author Unknown
5/1/2014 - Pending	Reviewed by ITS Security Team, CIO, ISO – Recommend Rewrite to comply with NIST Level 2
12/1/2014	Reviewed. Content suggestions. Added comments– Hien Huynh
3/2/2015	Minor Edits – Cleaned up for Draft Standard Posting on Web – Mike Cook
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
3/8/2019	Minor Edits –Incorporate additional two characters, increase lockout time by one minute and Duo 2FA password expiration – Hien Huynh

## Table of Contents

---

Executive Summary.....	2
Introduction and Purpose.....	5
Scope .....	5
SJSU Password Standard .....	5
Length and Complexity .....	5
Expiration .....	5
Account Lockouts .....	5
Reusing Passwords.....	5

## Introduction and Purpose

---

This standard defines the password requirements surrounding the management of access to information on San Jose State University's (SJSU) computer and communication systems. The purpose of this standard is to define security protection controls that will help minimize the loss of confidentiality, integrity, and availability of SJSU business information as it is stored, processed, and transmitted.

## Scope

---

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of SJSU Information Technology employees and partners. This standard applies to all passwords which grant access to confidential Level 1 and Level 2 data.

Wherever possible, this standard must be followed when configuring access control systems. Systems which cannot implement this policy must be approved and documented by the Information Security Office.

## SJSU Password Standard

---

### Length and Complexity

- Passwords must be between 10 and 28 characters.
- Passwords 10-16 characters in length
  - Must contain one Upper Case Letter (A-Z)
  - Must contain one Lower Case Letter (a-z)
  - Must contain one Number (0 through 9)
  - Must not contain a word listed in the SJSU Password Dictionary
- Passwords 17-28 Characters in length
  - No character restrictions

### Expiration

All passwords by default shall expire every 180 days.

All passwords for users enrolled in Duo 2FA shall expire every 2 years.

### Account Lockouts

Accounts shall be locked out after 5 consecutive failed login attempts. Lockout duration shall be at least 21 minutes.

### Reusing Passwords

Passwords can be re-used following five password resets.