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 breaches 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

<table>
<thead>
<tr>
<th>Standard #</th>
<th>IS-AC</th>
<th>Effective Date</th>
<th>Email</th>
<th>Contact</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>IS-AC</td>
<td>11/10/2015</td>
<td><a href="mailto:security@sjsu.edu">security@sjsu.edu</a></td>
<td>Information Security Office</td>
<td>408-924-1530</td>
</tr>
</tbody>
</table>

Policy History

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/30/2013</td>
<td>Updated/Posted – Standard appended to allow 16-28 character passwords by ISO – Original Author Unknown</td>
</tr>
<tr>
<td>5/1/2014</td>
<td>Reviewed by ITS Security Team, CIO, ISO – Recommend Rewrite to comply with NIST Level 2</td>
</tr>
<tr>
<td>12/1/2014</td>
<td>Reviewed. Content suggestions. Added comments – Hien Huynh</td>
</tr>
<tr>
<td>3/2/2015</td>
<td>Minor Edits – Cleaned up for Draft Standard Posting on Web – Mike Cook</td>
</tr>
<tr>
<td>11/10/2015</td>
<td>Incorporated changes from campus constituents – Distributed to Campus.</td>
</tr>
<tr>
<td>3/8/2019</td>
<td>Minor Edits – Incorporate additional two characters, increase lockout time by one minute and Duo 2FA password expiration – Hien Huynh</td>
</tr>
<tr>
<td>11/18/2020</td>
<td>Reviewed. Nikhil Mistry</td>
</tr>
<tr>
<td>2/24/2021</td>
<td>Updated/Posted - Standard updated to include new NIST and CO guidelines, 15 character length minimum standard, updated complexity requirement, and clarified dictionary check process.</td>
</tr>
<tr>
<td>10/19/2021</td>
<td>Reviewed. Cole Gunter</td>
</tr>
</tbody>
</table>
# Table of Contents

- Executive Summary 2
- Introduction and Purpose 4
- Scope 5
- SJSU Password Standard 5
  - Length and Complexity 5
  - Expiration 5
  - Account Lockouts 5
  - Reusing Passwords 5
  - Password Checks 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 15 - 72 characters
- Capital Letters, Numbers, Spaces and Special Characters are optional

Expiration
- All passwords shall expire every 2 years by default
- All passwords for users, delegated, and other non-standard accounts NOT enrolled in Duo Multi Factor Authentication (MFA) shall expire every 180 days

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 6 password resets.

Password Checks
Passwords shall be validated against Password Dictionaries to identify and deny easily crackable passwords, and passwords linked to credential dumps.