Standard: Multi-factor Authentication

Executive Summary

Passwords are the first line of defense for the computers, communications systems, and information security at SJSU. However, Multi Factor Authentication (MFA) is a necessary second line of defense. While complex, hard to guess passwords are critical for the security of our data and our systems, passwords are no longer deemed enough protection against modern security threats. The MFA standard defines the controls that will be required to implement and maintain an effective Multi Factor Authentication environment to increase the steps involved with account authentication while balancing the principles of confidentiality, integrity and availability.

Table of Contents

Introduction and Purpose

The purpose of this standard is to define requirements for accessing San Jose State University (SJSU) computer systems containing sensitive data from both on and off campus. The standards set forth in this document are intended to minimize potential security risks which may result from unauthorized use of SJSU computing resources. Multi-factor authentication adds a layer of security which helps deter the use of compromised credentials.

Scope

This standard applies to all SJSU faculty, staff, auxiliary employees, graduate assistants, student employees, students, volunteers, and vendors with access to SJSU systems.

This standard applies to any system that requires an additional layer of protection as determined by the SJSU IT Security Team in collaboration with campus data stewards. Systems requiring multi-factor authentication include those supported by SJSU Information Technology as well as systems administered by non-centralized departmental IT staff. Systems requiring the use of multi-factor authentication include, but are not limited to, virtual private network (VPN), systems utilizing Single Sign-On (SSO), system administration tools, and privileged accounts.

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

SJSU Multi Factor Authentication Standard

User requirements

1. Register a device that can receive push notifications or codes via the Duo Mobile app OR request a Key Fob during registration.

2. When users attempt to log into a SJSU computer system protected by multi-factor authentication, the system will “challenge” the user by requesting a second factor of authentication. This second factor could be an acknowledgement of a push notification, a code, or a physical token. This second factor will be provided through the secure method(s) the user selected during registration.

3. It is the user’s responsibility to promptly report compromised credentials to the SJSU IT Information Security Team.

Registration

Users will use the multi-factor authentication self-enrollment process to register their authentication device(s) and install the Duo Mobile app. More information is available on the SJSU Duo webpage.

Devices

Users may choose to deliver access codes and/or push notifications via the Duo Mobile app, which can be installed on any supported smartphone or tablet. The Duo Mobile app is the preferred and recommended solution for SJSU users. Users are encouraged to use personally owned or SJSU provided smartphones or tablets for the Duo Mobile app. The use of jailbroken/rooted devices is prohibited.

In addition, users have the option for accessing Duo multi-factor authentication codes via a code-generating token that can be provided by the SJSU IT Service Desk during the registration process. SMS is not currently an option for users to receive Duo codes for SJSU. Duo may, at its discretion, drop app support for older versions of mobile operating systems. Duo maintains the full list of supported devices.

Lost or Stolen Devices

If a user's registered device is lost or stolen the user should contact the SJSU IT Service Desk.

Off-Hours and Emergency Access to Protected Data

The SJSU Information Technology Division shall maintain internal procedures for processing emergency access requests if issues arise with the multi-factor authentication process. Users should contact the SJSU IT Service Desk for access.

Exclusions or Special Circumstances

There may be situations in which a member of the SJSU community has a legitimate need to utilize SJSU technology resources outside the scope of this policy. The IT Security Team may approve, in advance, exception requests based on balancing the benefit versus the risk to SJSU. Exception requests must be made through requests to the user's Campus Tech or the SJSU IT Service Desk. Policy exception requests shall be made to the SJSU IT Security Team and include a brief description of the system and/or type of data access requested. Please be certain to indicate if the user handles Personally Identifiable Information (PII) or other confidential information, such as electronic protected Health Information (ePHI), financial data, student academic records (e.g. grades or test scores), credit card payments, Social Security numbers, or works with children.

Due to the evolving nature of technology, cyber threats, and the changing roles of users at SJSU, all exemptions will be reviewed periodically and at the discretion of the IT Security Team in collaboration with data stewards. This review will verify that the need stated in the request is still valid and/or that the user still requires the approved multi-factor exempted access.

Information Security Standards

SJSU Multi Factor Authentication Standard

Standard #	IS-MFA	Effective Date	6/11/2021	Email	security@sjsu.edu
Version	2.0	Contact	SJSU IT Information Security Team	Phone	408-924-5555

Revision History

Date	Action
2/18/2021	Draft Created - Standard defined and described as currently implemented. Michael Hastings
2/22/2021	Reviewed by ITS Security Team, CIO, ISO
6/11/2021	Document finalized with minor changes and published by Information Security Officer
11/18/2020	Reviewed. Nikhil Mistry
10/4/2021	Review and update. Revision History Page.Janice Lew
11/3/2021	Reviewed. Cole Gunter
10/3/2022	Reviewed and Updated. Cole Gunter
6/27/2024	Reviewd and updated - Noel McCormick