Saint Mary's College of California
Information Technology Policy

Information
Technology Services

Multi-Factor Authentication Policy

Policy:	No: 2.0
Responsible Officer:	Chief Information Officer, James Johnson
Effective Date:	June 18, 2024
Updated:	August 27, 2024
Issued By:	ITS - Information Technology Services

CONTENTS

1.0 Purpose

Two-factor authentication (2FA), a subset of multi-factor authentication (MFA), is implemented to bolster the security of Saint Mary's College of California's (SMC) network accounts, aligning with National Institute of Security Technology (NIST) guidelines. This secondary authentication layer ensures protection against unauthorized access, especially in scenarios where passwords are compromised. SMC relies on Microsoft Authenticator as its current two-factor authentication solution.

Microsoft Authenticator, in accordance with NIST recommendations (NIST SP 800-63-3), provides a second authentication layer through either a mobile app or a hardware token, with a preference for the mobile app. All SMC users are required to register at least one authentication method in Microsoft Authenticator to access protected systems or applications. The use of Microsoft Authenticator for two-factor authentication is mandatory for all SMC systems and applications safeguarded by Microsoft Authenticator, adhering to NIST SP 800-53.

2.0 Accountability

Ensuring compliance with this policy falls under the purview of the President, the Chief Information Officer, and the President’s Cabinet, in line with NIST SP 800-53. Vice Presidents, Directors, and other managerial roles are responsible for implementing and supporting this policy within their respective areas, following NIST SP 800-37.

3.0 Applicability

This policy is applicable to all SMC faculty, staff and students as well as external entities utilizing SMC systems and applications protected by Microsoft Authenticator two-factor authentication, aligning with NIST SP 800-171.

4.0 Authentication Methods Insight

a. **Two-factor authentication (2FA):** Adds a second layer of security to an SMC Network Account, mitigating unauthorized access even if the password is compromised, aligning with NIST SP 800-63B.
    i. Two-factor authentication (2FA) is a subset of multi-factor authentication (MFA). MFA is a security process that requires users to provide two or more verification factors to gain access to a system or application.

b. **Microsoft Authenticator App**: Available on smartphone devices, it provides a second factor of authorization for Microsoft Authenticator-protected services, aligning with NIST SP 800-63B.

c. **Hardware token :** A small device generating a passcode for use as a second factor of authorization, in line with NIST SP 800-53.

5.0 Policy

1. SMC mandates all faculty, staff, students and external affiliates to use either the Microsoft Authenticator Mobile app or a hardware token for two-factor authentication, following NIST SP 800-63-3.
2. 2FA Considerations
    a. Mobile phone or tablet PUSH notifications are the recommended method for Microsoft Authenticator 2FA.

I. SMS Authentication Important Security Notice: Due to phishing threats via SMS, other words known as “Smishing” - you will not receive authentication notifications via text messaging.

b. Incompatible technology users, including faculty, staff, and students, can request a hardware token.

I. Requests for hardware tokens must be made to IT Services by contacting the Service Desk at 925-631-4266, itshelp@stmarys-ca.edu or by submitting a ticket through the IT Services portal. Each request will be reviewed by the Information Security team. Approval is contingent upon a risk-benefit analysis.

II. If a hardware token is lost or stolen, it must be reported immediately to IT Services at 925-631-4266, itshelp@stmarys-ca.edu or by submitting a ticket through the IT Services portal. The device will be deactivated to prevent unauthorized access to SMC’s authentication services. Individuals who are issued a hardware token are responsible for securing the token to prevent loss or theft. A replacement fee of $15.00 will be charged for any lost or stolen hardware token, payable by the individual, individual’s department or business unit.

III. Hardware tokens are the property of Saint Mary’s College of California and must be returned under the following conditions:

- Upon separation from employment at SMC
- When a student leaves SMC
- Upon request by the CIO or Information Security team

IV. It is important to note that personal hardware tokens not provided by SMC cannot be integrated into the SMC system and are not usable for MFA purposes.

c. SMC External partnerships and prospective students will be asked to authenticate via email.

6.0 Compliance

Violators may face the removal of system access or disciplinary action, including termination of employment at SMC.

7.0 Definitions of Key Terms

Term	Definition
Control	Actions taken or measures put in place to mitigate a risk.
Defacements	is an attack in which bad actors delete or modify the content on the SMC owned websites, replacing it with their own messages.
Division	A unit of the college headed by a VP, Chief, Dean or Director
Executive management	Senior Staff & President's Cabinet
Hardware Tokens	Hardware tokens are small "key fob"-size devices that have a LCD screen and display a rotating number when a button is pressed called a PIN. When authenticating using a security token, the user will be prompted to enter the PIN displayed on the token's screen.
Information Owners	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
NIST	National Institute of Standards and Technology
Visitors or External Partnerships	Non-SMC Employees (Consultants & Contractors)
SMS	Short Message Service (Text Messaging) for sending 160-character text messages

8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:
Saint Mary's College of California
1928 St. Marys Rd.
Moraga, CA 94575

9.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
7/29/2024	Publish	James Johnson
8/30/24	Hardware token policy updates	James Johnson