Saint Mary’s College of California
Information Technology Policy

Information
Technology Services

Password Policy

Policy:	No: 1.0
Responsible Officer:	Chief Information Officer, James Johnson
Effective Date:	May 1, 2024
Updated:	May 1, 2024
Issued By:	ITS - Information Technology Services

CONTENTS

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of an entire network. As such, all employees, including contractors and vendors with access to

Saint Mary's College of California network and systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their password. Many attributes of this password regulation follow NIST's (National Institute of Standards and Technology) recommendations on password management.

2.0 Password Minimum Requirements

To protect the security of the College's systems and data, all users are required to use strong passwords following these guidelines:

a. Passwords must be at least 16 characters long.

b. Passwords must contain a combination of at least three of the following character types:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numerals (0-9)
- Special Characters (e.g. !, @, #, $, %, etc.)

c. Avoid using common dictionary words, names, or easily guessable patterns.

- WelcometoMyHouse, GoodnightToAll
- James6677889900, Karen987654321
- 12345aaaa12345aaaa, 123456789876543

2.1 Password Expiry and Renewal

a. Passwords must be changed once a year.
b. Users cannot reuse the same password.

Students are encouraged to do the same but are not required currently. Any password used for access to Saint Mary's College IT resources should be unique and not used for access to any other site or application.

2.2 Password Storage and Transmission

a. Passwords must not be stored in plain text and must be stored securely using cryptographic hashing algorithms.
b. Encrypted transmission protocols (e.g., HTTPS) must be used for transmitting passwords over the network.

2.3 Account Lockout Policy

a. Accounts will be locked out after six consecutive failed login attempts.

b. Users must contact the IT Department to unlock their accounts in case of lockout or the account will be unlocked after 15 minutes.

3.0 Password Security Best Practices

a. Do not share passwords with anyone, including colleagues or IT personnel.
b. Do not write passwords in easily accessible locations (e.g., on sticky notes, in desk drawers, etc.)
c. Never provide passwords over e-mail or any other non-secure communication channels.
d. Passwords used for work accounts should not be used for personal accounts and vice versa.

3.1 Multi-factor Authentication (MFA)

a. Multi-factor authentication will be implemented whenever possible to add an extra layer of security.

3.2 Exceptions

Passwords may be revealed under certain circumstances to the following:

a. Law-enforcement agencies and courts requesting information under court orders and rules of evidence that require disclosure.

b. Supervisors needing access to an employee's account after they have departed from St. Mary's College of California. HR needs to be notified and written approval is needed and recorded.

4.0 Compliance and Enforcement

a. All Saint Mary's College of California employees are required to comply with this policy.
b. Violations of the password policy may result in disciplinary action depending on the severity of the violation.

5.0 Periodic Review

a. The password policy will be periodically reviewed and updated to incorporate changes in security best practices and technological advancements.

6.0 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

7.0 Revision History

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

Date	Description of Change	Reviewer
5/1/2024	Publish	James Johnson