Saint Mary's College of California
Information Technology Policy

Information
Technology Services

Fictitious Email Account Policy

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

CONTENTS

1.0 Purpose and Justification

The purpose of this policy is to establish guidelines for the creation, use, and management of fictitious email accounts. These accounts are used both for internal purposes such as testing and training, as well as for external communication with the public. Examples include email addresses like or **commencement@stmarys-ca.edu** or **apply@stmarys-ca.edu** which serve as points of contact for general inquiries or specific business operations.

Each request for a fictitious account must provide a clear justification for why it is needed, especially in cases where multiple accounts are requested. For example, if a department requests several public-facing accounts, they must explain the intended use and benefit to the college.

2.0 Eligibility and Approval

A. Staff or faculty can request fictitious email accounts.
B. Student clubs can request a fictitious account with approval from the Student Involvement Leadership team.
C. On-campus vendors may be granted a fictitious account after review.
D. All requests must be approved by the head of the department and the CIO.
E. Requests for accounts intended for public use (e.g., customer service, general inquiries) must include details on the expected use case.
F. All requests must be submitted through the IT Services ticketing system with proper justification.

3.0 Account Ownership and Responsibilities

A. A **Primary Owner** must be designated for each fictitious email account or set of accounts. The Primary Owner is responsible for:

i. Managing the account and ensuring it serves its intended function.
ii. Ensuring security protocols are followed.
iii. Monitoring the account for any misuse or errors in communication.
iv. Reviewing accounts regularly to ensure timely responses.
v. Resetting passwords annually.
vi. Requesting deactivation or reassignment of accounts when users leave the college or their position.
vii. Reassigning their primary ownership, in coordination with IT Services, when they are no longer working at the college.
viii. Not sharing passwords and setting up delegation for the account if access needs to be granted to others.
ix. Delegating access to the email account to other users as needed, ensuring

secure and compliant access in accordance with organizational policies.

x. Ensuring multi-factor authentication (MFA) is properly set up and maintained for the account, in compliance with security policies.

xi. Deleting delegated accounts when a user leaves.

4.0 Account Request Process

A. All fictitious email account requests must be submitted through the IT Services ticketing system.

B. Requests must include clear justification, details on the purpose of the account, and any special considerations (e.g., public use or specific routing needs).

C. Approval from the department head and CIO is required before the account can be created.

5.0 Security Requirements

A. **Passwords** for all fictitious email accounts must be strong and reset annually.

B. **Multi-Factor Authentication (MFA)** is required for all fictitious email accounts, regardless of whether they are used internally or for public communication.

C. **Passwords must not be shared**. Each fictitious account should have a responsible Primary Owner managing it securely.

D. **Upon the departure of the Primary Owne**r, the account should be deactivated or reassigned immediately. The Primary Owner is responsible for contacting IT Services to reassign. The Primary Owner should not reassign the account without making IT Services aware of the change.

6.0 Public Use Guidelines

A. Fictitious email accounts intended for public communication (e.g., customer support, general inquiries) must be monitored regularly to ensure timely responses.

B. These accounts must not be used for personal or unauthorized communication.

C. Public-facing accounts should be configured with automatic replies or routing rules where necessary, ensuring that inquiries are addressed promptly.

7.0 Naming Conventions

A. **Descriptive and Clear**: The account name should reflect its purpose or function, so anyone interacting with it knows the type of communication they are addressing.

B. **Consistency**: Use the same format across all fictitious accounts to maintain uniformity.

C. **Avoid Personal Names**: Avoid using real names unless the account is meant to represent a department or a role (e.g., dean@stmarys-ca.edu).

D. **Branding Considerations**: Ensure the names align with the organization's branding and communication guidelines. Naming conventions may be reviewed by The Office of Marketing and Communications to ensure they align with the institution's communication and branding standards.

E. **Naming Conventions Guidelines**
    a. **Public Communication Accounts:** For accounts that interact with the public (e.g., customer support, business inquiries):
        i. **Function + Domain**: Use the specific function followed by the domain.
            1. Example: support@stmarys-ca.edu, info@stmarys-ca.edu.
        ii. **Team Name + Function**: Reflect both the team and the role of the account.
            1. Example: admissions-support@stmarys-ca.edu, hr-info@stmarys-ca.edu.
        iii. **General Queries**: Keep it broad for general public inquiries.
            1. Example: getinfo@stmarys-ca.edu, questions@stmarys-ca.edu.
    b. **Testing Accounts:** For accounts used in testing or for internal purposes:
        i. **Prefix + Department + Purpose**: Use a clear prefix like "test-" followed by the department and purpose.
            1. Example: test-finance-report@stmarys-ca.edu, test-it-deploy@stmarys-ca.edu.
        ii. **Numbered Variants**: For multiple test accounts, use sequential numbering or dates.
            1. Example: testuser1@stmarys-ca.edu, test-account2024@stmarys-ca.edu.
    c. **Anonymized / Role-based Accounts:** For accounts used by specific roles without tying them to an individual:
        i. **Role + Department/Function**: Indicate the role followed by the department or function.
            1. Example: dean-office@stmarys-ca.edu, editor@stmarys-ca.edu.
        ii. **Service-Oriented Accounts**: Focus on the service being offered.
            1. Example: servicedesk@stmarys-ca.edu, billing@stmarys-ca.edu.
    d. **Temporary or Project-Based Accounts:** For short-term accounts tied to a specific project or event:
        i. **ProjectName + Function**: Clearly identify the project followed by the role or purpose.
            1. Example: event2024-support@stmarys-ca.edu, project-x-lead@stmarys-ca.edu.

        ii. **Dates or Versioning**: Include the project’s timeline to help track temporary usage.
            1. Example: event-q1-2024@stmarys-ca.edu, beta-test-2024@stmarys-ca.edu.
    e. **Multi-Functional Departments:** For departments with multiple purposes or sub-teams:
        i. **Department + Function**: Reflect both the department and the specific role or function.
            1. Example: mfa-dance@stmarys-ca.edu, mfa-communications@stmarys-ca.edu.
        ii. **Team-Specific Accounts**: If the department has sub-teams, you can differentiate with further details.
            1. Example: admissions-grad@stmarys-ca.edu, admissions-undergrad@stmarys-ca.edu.

8.0 Review and Audit of Accounts

A. The need for each fictitious account, especially those with public-facing roles, will be reviewed periodically to ensure they are still necessary and functioning correctly.
B. Departments requesting multiple public-facing accounts must provide detailed justification for their request, which will be subject to additional assessment during the review process.

9.0 Penalties for Misuse

Any misuse of fictitious email accounts, including violating security policies or using accounts for unauthorized purposes, will result in disciplinary action in accordance with the college’s IT and security policies.

10.0 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

11.0 Revision History

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

Date	Description of Change	Reviewer
11/11/2024	Publish	James Johnson