Faculty & Staff Email

Division:
Administration & Finance

Department:
Information Technology Services

Effective Date:
Wednesday, May 11, 2016

Revised Date:
xx,xx,xxxx

Authority:
ICSUAM 8105
ICSUAM Policy Section 8000 Information Security

Objective:
This Practice Directive defines service offering, requirements and provisions governing the use of faculty, staff, community members, and emeriti email services provided by SF State.

Statement:

Purpose and Scope
This Practice Directive defines service offering, policies, requirements, and provisions governing the use of faculty and staff email services provided by San Francisco State University. SF State supports one enterprise email system providing all faculty, staff, community members, and emeriti with an @sfsu.edu email account for official University communications.

Eligibility
Current faculty and staff (employees) as defined by Human Resources, community members, and emeriti are eligible for email services.

Primary Account
All SF State employees are required to have an SF State email account to receive official University communications, and are required to use it for all email communications to conduct SF State
business. The account directly associated with the user’s SF State ID and login credentials is considered a primary email account and will be used for official University communications.

**Aliases**

Up to five email aliases are available for multiple sending addresses for a given primary email account (e.g. where messages that are sent to the alias will be received in the primary account inbox).

**Secondary Accounts**

*Individual Accounts*

Up to five secondary email accounts may be provided to faculty members and administrators for eligible use cases, such as when the account holder requires separation between messages directed to different addresses. Secondary email accounts cannot be substituted for primary email accounts.

*Departmental Accounts*

Departmental accounts are a type of secondary email account that are associated with a department, college, or program rather than an individual. Ownership of a departmental email account is held, by default, by the department, college unit or program head (such as department chair, director, or dean) regardless of who requested the departmental email account.

**Suspending/Deleting Accounts (De-provisioning)**

An email account will be suspended or deleted according to the following procedures:

1. Standard employment termination or discontinuation of community member status: Users who do not have a current faculty, staff, community member, or emeritus status will have their email accounts deleted
2. Secondary email accounts will be deleted when all owners and co-owners are no longer affiliated with SF State
3. A violation of the SF State Responsible Use Policy may result in a suspension or deletion of an email account
4. Email accounts may be suspended, deleted, or reassigned when an official request is received from Human Resources (HR), University Police Department (UPD) or University Counsel

**Email Account Names**

For ease of email account provisioning across systems, email account names shall be 2-32 characters in length.

Email account name (short name) changes are available on an exception basis only, such as for legal name changes.

Following the deletion of a primary email account, an email account name will not be reassigned for 6 months.

Email account names must be compliant with the SF State Responsible Use Policy and the SF State Principles of Conduct in a Multi-Cultural University Practice Directive.

**Campus-wide Email Directory**
Campus email users’ names and email addresses will be displayed in the email directory. Users may select and set a “preferred” email directory name they wish to display online instead.

Mass (Bulk) Emails

Mass emails are defined as email messages sent to a large group of recipients such as, but not limited to: all students, all faculty and/or all staff. Messages intended for distribution to all students, all faculty and/or all staff groups require VP or Presidential approval. SF State email services have limitations on the number of emails that can be sent from individual primary or secondary email accounts. For large volume email communications exceeding those limits, users should use Campus designated and approved mass email services. Mass email campaigns should follow SF State Email Standards for message security and formatting.

Forwarding

Automated forwarding of SF State email accounts to non-SF State Services is not supported. This is to ensure SF State is able to meet compliance requirements for email management and when necessary, can respond to Public Records Requests (PRAs) and apply controls such as litigation hold to SF State emails. In addition, this reduces risks of sensitive data disclosure.

Security

Access

Passwords are considered Level 1 data should not be stored in email clients. SF State requires the use of approved email clients that support modern authentication protocols with strong encryption and email clients must be compatible with SF State 2 Factor Authentication (2FA).

Securing Content

Users should follow established campus security practices for sharing sensitive information. Unencrypted email messages are not a secure form of communications. Sensitive information, such as electronic Protected Health Information, Personally Identifiable Information and PCI-DSS card data should not be communicated via unencrypted email.

Implementation

Responsibility for implementing this Practice Directive will rest with Information Technology Services (TS). Submit any apparent violation of Faculty and Staff Email Practice Directive to the appropriate administrative authority (vice president, dean, director, department, or program chair) or to service@sfsu.edu.

Non-Compliance

Non-compliance with applicable policies and/or practices may result in suspension of email access privileges. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.