4-OP-H-13 Electronic Mail Policy

Responsible Executive: Finance and Administration

Approving Official: Vice President for Finance and Administration

Effective Date: March 24, 2020

Last Revision Date: New: July 12, Technical Change-June 14, 2020 , Amended 06/03/2022

I. INTRODUCTION

Florida State University provides electronic mail (email) services and accounts for employees, students and others to support the university's mission. This policy is intended to outline requirements and guidelines associated with email account use and administration.

II. POLICY

A. Overview

Email is a fundamental communication tool for the university. As such, email services are provided and managed by Information Technology Services (ITS) to ensure email is available, reliable and secure. FSU's email system is the official means of communication for university business for employees and students. Users are required to conduct FSU business from their FSU assigned email address containing the fsu.edu domain.

B. Definitions

Email Account Username – the primary identifier assigned to and used for accessing the email mailbox.

Email Address – an email name used to send and receive email.

Email Domains – a domain name that is uniquely associated with a university unit recognized by the FSU Board of Trustees. The primary domain is fsu.edu. Secondary domains, such as med.fsu.edu and wfsu.org, are generally used for

marketing or identification purposes, i.e. demonstrate one or more persons are associated with a specific unit.

Email Alias - a secondary name that identifies the person (account holder) and is used within an email address, e.g. aliasusername@fsu.edu.

Private – the classification of data for which the unauthorized disclosure may have moderate adverse effects on the university's reputation, resources, services, or individuals.

Protected (Confidential) – the classification of data deemed confidential under federal or state law or rules, FSU contractual obligations, or privacy considerations such as the combination of names with respective Social Security numbers. Protected data requires the highest level of safeguarding protection.

Public – the classification of information for which disclosure to the public poses negligible or no risk to FSU's reputation, resources, services, students or employees. Due to State of Florida public records laws, this is the default data classification, and should be assumed when there is no information indicating that data should be classified as private or protected.

Public Records - (as defined by Chapter 119, F.S.) Public records are all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business. A particular record may contain some information which is public under law, some which is exempt from mandatory disclosure but might be disclosed and other which is legally confidential. When unclear, such determinations as to a particular record disclosure should be made by the University Attorney.

Records Retention Schedule - A standard approved by the Florida Department of State, Division of Library and Information Services, for the orderly retention, transfer or disposal of public records taking into consideration their legal, fiscal, administrative and historical value.

Retention - The minimum time period necessary to retain records before they have met their administrative, legal, fiscal or historical usefulness, as set forth by the Florida Department of State, other regulations and contractual requirements.

Spam - Unwanted and unsolicited email or material created or knowingly disseminated in such a large volume that it tends to disrupt the proper functioning of university information technology resources or individuals' ability to use such resources. Spam is most often sent to a large number of email accounts and may be used to deliver malware and/or links to malicious websites.

C. Scope

This policy applies to all persons associated with the university who use, administer, manage, or maintain FSU email, their supervisors, and their unit administrators.

D. Assignment of Email Accounts and Access to Email Accounts

FSU employees, students, retirees and active courtesy appointees receive email accounts provided by ITS to be used for conducting official university business. ITS also provides email addresses and accounts to support communications with groups of people, applications and systems.

The default email address includes @fsu.edu. Employees may use an email alias and additional email domain name as an alias email address. To ensure successful delivery of university email, the designated @fsu.edu email address will be used for official university business communications and configured to be used in university applications and systems, such as OMNI.

Retired employees may continue to use their @fsu.edu email account upon retirement from the university. Such use by retired employees may be discontinued for (1) inactivity as provided herein or (2) misuse as provided by university policy or law e.g., commercial use, system damaging use, etc. Requests may be submitted by the retired employee, or for retired staff employees by the department or university, as provided herein, to disable access to @fsu.edu email account. Retired employees that continue to have access to

their @fsu.edu email account will maintain access unless the account is inactive for a one-year period. At such point, the retired employee will then be contacted using all email addresses on file for them to request that the account be accessed for another year. After the inactivity notification the retired employee will have thirty (30) additional days to provide notice to the university before the account will be disabled.

Unless a former employee has been granted continued email account access for reasons other than retirement, when an employee separates from FSU, the following actions are generally taken unless the employee is currently classified as a student:

- Access to the email account by the employee will be disabled
- The contents of the email account will be preserved
- The dean, department head, director may request access to a filtered copy of the mailbox for historical reference; the contents released to the department will be based on approved search criteria provided by the requesting unit, and the former employee will be informed of this request.
- By default, a standard reply message will be constructed to let others know that the employee is no longer with the university. This message will provide the following information:
    - the person no longer is associated with the university
    - the email account is not monitored
    - standard reply message will expire after one year
- The dean, department head, director, or unit IT manager may request additions to the automatic reply message to be sent on behalf of the account. These edits may contain:
    - an email address where university business correspondence should be sent
    - With the employee's permission, an email address where non-university (personal) correspondence may be sent

The following actions are generally taken for separated students, unless the student is also an employee or former employee in which case the email account will be treated as an employee or former employee account:

- Access to the email account of the student will continue until for a period of time specified by email standards.
- The contents of the email will be removed, and the email account deleted after the specified period
- If the student returns on a later date, the email account will be recreated with the same email address as before and no previous data will be available

E. Email Use

Employees, students and others considered to be the primary account holders are responsible for email messages originating from their accounts.

Employees must use email in a responsible, effective, and lawful manner.

To ensure compliance with various laws and regulations and to ensure university business records are otherwise properly retained @fsu.edu email accounts must be used for correspondence associated with an employee's job duties. ITS will not use server forwarding rules to forward or automatically redirect employee emails to a non-FSU (private) email system or account, such as gmail.com, yahoo.com, comcast.net, etc. Protected (confidential) and private information should be encrypted or password protected when transmitted via email. University email accounts may not be used to send spam.

F. Email, Public Records and Retention Requirements

University @fsu.edu emails sent or received in connection with official university business are public records and must be managed in accordance with applicable laws, regulations, and university policies.

Email is generally considered a protected data asset and is maintained in the most secure manner possible. Access to the email system is limited to a

minimum number of trusted employees and access to email account is governed by the Information Security Policy 4-OP-H-5. Specifically, access to email is restricted per policy: "Monitoring, sniffing, and related security activities shall be performed only by authorized workers based on job duties and responsibilities, by members authorized by the Director of ISPO, or unless necessary for academic instruction or research and approved by the director of the unit that supports the system."

Email retention and classification (public, private, or protected) requirements are based on the information contained in emails and as defined by university policies, federal and state laws and regulations, contracts and other legal arrangements.

Destruction of emails shall be in compliance with the records retention schedule (**https://recordsmanagement.fsu.edu/records-schedule (https://dos.myflorida.com/library-archives/records-management/general-records-schedules/)**) and other applicable rules and regulations associated with research grants, etc.

G. Implementation

Effective Date: To be determined upon adoption of the policy by university administration

H. Policy Review and Update

This policy shall be reviewed and updated as special events or circumstances dictate.

III. LEGAL SUPPORT, JUSTIFICATION, AND REVIEW OF THIS POLICY

OP-F-3 Records Management

OP-H-5 Information Security Policy

OP-H-12 Information Privacy Policy

BOG Regulation 3.0075 Security of Data and Related Information Resources

Florida Statutes Chapter 119 Public Records

Florida Statutes Chapter 815 Computer-Related Crimes