FLORIDA STATE UNIVERSITY

4-OP-H-13 ELECTRONIC MAIL POLICY

Responsible Executive: Vice President Finance and Administration
Approving Official: Vice President Finance and Administration
Effective Date: On approval and notice
Revision History: New-

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 provide requirements and guidelines associated with email account use and administration.

II. POLICY (Including any Forms and Attachments)

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 services are available, reliable and secure. ITS is the only provider of university employee and student email accounts and is authorized to develop procedures and guidelines for the use of all university email systems.

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 Username - a secondary name that identifies the person (account holder) and is used within an email address, e.g. alias_username@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.

FSU public record classifications of protected, private, or public (see definitions) determine whether and with whom certain records may be shared.

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 – Irrelevant, inappropriate or unsolicited emails that are not directly related to the recipients, an employee's responsibilities, student academic and university experience or other legitimate university-related purpose. 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, certain contractors 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. Applications and systems requiring their own email systems are permitted if systems are secured and compliance with relevant records retention and legal requirements are ensured.

The primary email address for employees includes @fsu.edu. Primary student account addresses include @my.fsu.edu. Employees may use an email username alias and secondary email domain name as an alias email address. To ensure successful delivery of university email, the designated @fsu.edu email address for employees and @my.fsu.edu address for students will be used for official university business communications and configured to be used in university applications and systems, such as OMNI.

Students employed by FSU will have two email accounts – a student email account for student-related communications, and an employee email account for use when a person is fulfilling their FSU employee role. Student email accounts should not be used as employee email accounts. Employee accounts should not be used as student accounts.

Retired employees may continue to use their @fsu.edu email account. Upon request by the employee, preferably prior to the time of the employee's separation, continued use of the email account will be permitted. If the account is inactive for a one-year period the retiree will be contacted using all email addresses on file to request that the account be accessed in order to continue access for another year. The retiree will have thirty (30) additional days after they are contacted to access the account before the account will be disabled.

Unless a former employee has been granted continued email account access, when an employee separates from FSU employment, the following actions are generally taken:

- 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 advised 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 will provide the following information:
    - the person no longer is associated with the university
    - the email account is not monitored
- 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. This 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

E. EMAIL USE

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

Employees should 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, university employee email accounts should be used for all 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. Employees may establish individual forwarding rules in their own email account settings. If an employee uses a private account for correspondence associated with an employee's job duties, either sent or received, the employee is required to copy relevant emails to the employee's primary university email account.

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

Employee emails sent or received in connection with official university business are most likely 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 (http://vpfa.fsu.edu/records-schedule) 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

/s/ Name of Approving Official

[Proof of approval retained in file]