OP-F/H-XX ELECTRONIC MAIL POLICY (version 1.2 xxx. 2016)

SPECIFIC AUTHORITY

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

I. OBJECTIVE

Florida State University provides electronic mail (email) to employees to support the University's mission. This policy is intended to provide guidelines for effective practices and processes to the users of FSU email.

A. OVERVIEW

Email is a fundamental business communication tool for University employees as well as certain contractors and visitors conducting business at FSU. Information Technology Services (ITS) is the only provider of FSU employee email accounts.

This policy provides procedures for these aspects of email accounts and use:

- Appropriate use of FSU email;
- Responsibilities associated with assigned email addresses and accounts;
- Assignment and termination of email accounts.

Information Technology Services (ITS) is authorized to develop procedures and guidelines for the consistent implementation of this policy.

B. DEFINITIONS

Approved Email Alias – an alternative email address assigned by ITS and used for FSU email.

Domain Name – a unique name used to identify university Internet-accessible resources, for example, fsu.edu, med.fsu.edu, wfsu.org.

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

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

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, or individuals. This is the default FSU 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.

Spam – unsolicited emails (or other messages) that are often sent out in bulk and used to distribute advertisements, but also increasingly used to deliver malware and/or links to malicious websites.

URL – Uniform Resource Locator; used to specify addresses on the World Wide Web.

Vanity Email Domain – a domain name that is uniquely associated with a university unit recognized by the FSU Board of Trustees. It is generally used for marketing or identification purposes e.g. med.fsu.edu, wfsu.org.

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

FSU employees, certain contractors and active courtesy appointees receive email accounts to be used for University business purposes.

Email accounts and addresses are provided by and administered by ITS. ITS is the only provider of employee email accounts. ITS will establish the naming standards for email accounts and addresses. ITS will create "vanity" email domains like unit1.fsu.edu only for colleges, departments, centers and institutes recognized and approved by the University Board of Trustees. Vanity email domains that existed prior to the enactment of this policy will be managed by ITS. Employees will be given the option of requesting aliases for vanity email domains.

Only email addresses provided by ITS are approved for use by employees conducting University business.

Email aliases may change as employees transition between different units using vanity email domain addresses. To ensure successful delivery of University email, the designated @fsu.edu email address for all employees will be used for official employee communications and configured to be used in University applications and systems, such as OMNI.

A student who is employed by FSU will have two email accounts – a student email account for student-related communications, and a faculty/staff email account for use when the person is fulfilling his/her FSU employee role. Student email accounts shall not be used as employee email accounts. Employee accounts shall not be used as student accounts.

E. EMAIL USE

FSU email is intended to support the University mission.
You are responsible for emails originating from your account.
Email should be used in a responsible, effective and lawful manner. The following should be considered:

- To ensure compliance with various laws and regulations and to ensure university business are otherwise properly retained, this policy prohibits automatically forwarding or automatically redirecting all incoming emails relating to university business to a non-FSU email system or account, such as gmail.com, yahoo.com, comcast.net, etc. Forwarding of individual messages is permitted although responses to university-related email should originate from the university email account rather than a non-university account that may contain a forwarded message. Former employees who are permitted to retain use of their address, such as some retirees, may automatically forward mail to a non-FSU account as it is expected such email will not be associated with university business.
- Employees who are also students shall not forward FSU business emails to student email accounts.
- Protected (confidential) and private information should be encrypted or password protected when transmitted via email.
- Do not send or forward emails with libelous, defamatory, offensive, racist or obscene remarks.
- Do not propagate "chain" emails, spam, etc.

F. EMAIL, PUBLIC RECORDS, AND RETENTION REQUIREMENTS

Emails sent or received in connection with official FSU business are public records and must be managed in accordance with applicable laws, regulations, and FSU policies.

Email retention requirements and classification (public, private, or protected) are based on the information contained in emails.

Destruction of emails shall be in compliance with the records retention schedule (http://vpfa.fsu.edu/records-schedule) and other applicable rules and regulation associated with research grants, etc.

G. EMAIL MONITORING

While FSU does not routinely monitor the content of email, the University may inspect, copy, store, or disclose the contents of email messages on University systems when these actions are appropriate to

- prevent or correct improper use of University email;
- mitigate network or endpoint device security violations;
- ensure compliance with University policies, procedures, or regulations;
- satisfy a public record request, court order, or in connection with legal proceedings;
- comply with a request of a law enforcement agency; or
- ensure the proper operations of the University.

Any emails or accounts found to be in violation of this policy may be turned over to University officials, law enforcement, officials of the court, or other officials engaged in an investigation.

H. TERMINATION OF UNIVERSITY EMAIL ACCOUNTS

When an employee separates from FSU employment the following actions are to be taken:

- Access to the email account by the employee will be disabled;
- The contents of the email account will be preserved;

- The supervisor, dean, department head, director may request mailbox access or a copy of the mailbox;
- The supervisor, dean, department head, director, or unit IT manager may request ITS enable an automatic reply message with the following information
  - that the person no longer is at FSU;
  - an email address where FSU business correspondence should be sent;
  - an email address where non-FSU correspondence may be sent.

Retired faculty members may retain @fsu.edu email upon request at the time of retirement.

To reduce possibility of misuse, in the case of employee termination or a death, email access will be disabled immediately.

I. IMPLEMENTATION

Effective Date: December XX, 2016

J. POLICY REVIEW AND UPDATE

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