Employee and Student Email Policy

I. POLICY STATEMENT

Auburn University email is an approved medium for communication among Auburn University employees, students and external parties.
Persons with Auburn University email accounts are expected to use them appropriately.

II. POLICY PRINCIPLES

The purpose of this policy is to ensure that Auburn University email is an effective and secure means of communication for Auburn University employees and students. Auburn University email systems are managed in accordance with the University's Electronic Privacy Policy. Email sent outside the university is not assured of privacy and may be viewed by others.

III. EFFECTIVE DATE

This policy replaces the former employee email policy, faculty email policy and student email policy and is effective October 31, 2016.

IV. APPLICABILITY

This policy applies to all Auburn University email accounts and the persons or entities to which they are assigned.

V. POLICY MANAGEMENT

Responsible Office: Office of the Chief Information Officer
Responsible Executive: Executive Vice President and Provost
Responsible Officer: Chief Information Officer

VI. DEFINITIONS

Confidential information

1. Auburn Confidential data is business or personal information that is required to be strictly protected. (See the Data Classification Policy for more information.)
2. Confidential information received by email may include personal data not relevant to the conduct of Auburn University business and should be deleted.

Auburn University email accounts are email accounts that have addresses ending in "auburn.edu."

Non-Auburn email account is any email account that is not an Auburn email account. The location of person using the account or equipment supporting the account is not a factor.

Email spoofing is the creation of **email** messages with a forged sender address.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. **Spear Phishing** is an email spoofing fraud attempt that targets a specific organization (Auburn University) and seeks unauthorized access to confidential data or funds. Often, the apparent source appears to be a known and trusted individual, there is information within the message that appears to support its validity, and the request the individual makes seems to have a reasonable basis.

VII. POLICY PROCEDURES

1. Official email communication for Auburn University employees and students should be made only through the Auburn email system. The use of non-Auburn email for sending confidential or sensitive Auburn University information is prohibited.

2. Auburn University employees and students are responsible for checking their Auburn University assigned email account with a frequency appropriate to the activities in which they are involved. If employees do not have computer access on the job, their supervisors shall inform these employees of all relevant official communications delivered via email.

3. No confidential Auburn University data (see Data Classification Policy) may be transmitted via email unless it has been rendered secure from unauthorized access.

4. If Auburn University employees receive confidential information via email or email attachments that is required for university records, the information must be saved to an approved secure location. Once the information has been saved, the email and the attachments should be permanently deleted.

5. If Auburn University employees receive confidential information via email or email attachments that is not required for university records, the information should be permanently deleted immediately.

6. Email communications with students should be addressed to their Auburn email address.

7. The originator of any Auburn University communications sent via email is responsible to determine and comply with archival requirements. See General Records Schedule for Alabama Universities for archival requirements.
   www.lib.auburn.edu/archive/records_schedule.htm

8. Email is not a replacement for officially required forms or procedures.

9. Email must be consistent with Auburn University policies, meet ethical conduct and safety standards and comply with applicable laws and proper business practices. State law prohibits the use of public resources in support of political candidates.

10. Email that is identified as a business record shall be retained according to Auburn University's Record Retention Schedule.

11. The Auburn University email system shall not be used for the creation or distribution of messages that violate the University's Policies Prohibiting Harassment of Employees or Students (see the Employee Harassment Policy, Student Harassment Policy, and Sexual and Gender-Based Misconduct Policy). Employees who feel they have suffered harassment via the Auburn University email system or by other means should report the harassment to the Office of AA/EEO & Title IX. An online complaint form can be completed here: Discrimination or Harassment Complaint Form.
    http://auburn.edu/administration/aaeeo/Policies.php

12. Employees are prohibited from automatically forwarding Auburn University email to a third party email system. Individual messages that are forwarded by the user must not contain Auburn University confidential or sensitive information.

13. Sending unauthorized mass mailings from an Auburn University email account is prohibited.

14. Auburn University does not guarantee privacy in anything stored, sent or received on the University's email system, as explained in the Electronic Privacy Policy.

15. If a user suspects their email account has been compromised, they should contact their IT provider or the OIT HelpDesk at (334) 844-4944.

16. Incidents of phishing should be reported to the OIT HelpDesk at (334) 844-4944 or spamreport@auburn.edu

VIII. SANCTIONS

Email accounts that are used in ways that violate this policy may be suspended.
Failure or refusal to comply with this policy may result in discipline up to and including dismissal.

IX. EXCLUSIONS

There are no exclusions to this policy.

X. INTERPRETATION

For interpretations of this policy refer to the Office of the Chief Information Officer.

Revised: March 15, 2006
Revised: October 21, 2016