# Auburn University at Montgomery
## Policies and Procedures

**Title:** E-Mail Policy

**Responsible Office:** Office of Technology

## I. PURPOSE

The purpose of the e-mail policy is to ensure the proper use of AUM's e-mail system and make users aware of what AUM deems as acceptable and unacceptable use of its email system.

## II. POLICY

E-mail is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of e-mail can post many legal, privacy and security risks, thus it's important for AUM end users to understand the appropriate use of electronic communications. This policy establishes e-mail as the approved medium for communications and outlines the minimum requirements for use of e-mail.

## III. EFFECTIVE DATE

December 1, 2017

## IV. APPLICABILITY

This policy applies to all AUM email accounts and the individuals or entities to which they are assigned

## V. RESPONSIBILITY

**Policy Responsible Office:** Office of Technology
**Policy Responsible Executive:** Chief Information Officer (CIO)

## VI. DEFINITIONS

**AUM employees** refers to all faculty, staff, and contracted personnel.

**Users** refers to all individuals or entities who have been assigned or have access to an AUM email address.

**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 (AUM) 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.

**SPAM**, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email. Many email spam messages are commercial in nature but may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments.

## VII. PROCEDURES

General:

1. All use of email must be consistent with AUM policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices. State law prohibits the use of public resources in support of political candidates.
2. AUM employees and students are responsible for checking their AUM 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. Email accounts are created once a student has been admitted at the University or an individual starts employment at AUM. The email username is based on the official name of the student or employee as reflected in the University student database (Banner). Requests for mail aliases based on name preference, middle name, nicknames, etc., cannot be accommodated. The only requests for display name change that will be processed are to correct a discrepancy between email display name and official University records, in which case the email display name will be corrected.
4. Sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is deemed to be authored by the account owner, and it is the responsibility of that owner to ensure compliance with University policies. Additional information regarding passwords can be found in the User Password Policy.
5. The AUM email account is the official method of communication from the University. Email communications with students should be addressed to their AUM email address. This policy is not intended to preclude or eliminate other approved means of communications such as BlackBoard's message feature.
6. Email is not a replacement for officially required forms or procedures.
7. The AUM email system shall not be used for the creation or distribution of messages that violate the University's policies regarding prohibiting discrimination & harassment of employees or students. Students or employees who feel they have suffered harassment via the AUM email system or by other means should report the harassment to the Office of Human Resources.
8. Sending unauthorized mass mailings from an AUM email account is prohibited. A list of various University distribution lists and authorized senders is maintained by ITS. Requests to send out university-wide messages may be directed at the Office of Strategic Communications and Marketing.
9. While AUM will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through the University system. With prior approval by the

Chancellor, AUM may monitor messages without prior notice but is not obliged to monitor email messages.

10. If a user suspects their email account has been compromised, they must contact the ITS Helpdesk at (334) 244-3500.
11. Incidents of phishing should be reported to the ITS Helpdesk at (334) 244-3500 or phishing@aum.edu.
12. While the incoming email is scanned for malware and for messages deemed to be 'SPAM', it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each user to use proper care and consideration to prevent the spread of malware. In many cases, malware appears to be sent from a friend or coworker, therefore attachments should only be opened when the user is sure of the nature of the message. If any doubt exists, the user should contact ITS or the sender to verify the authenticity of the message and/or the attachment.
13. AUM owns all email accounts and all data transmitted or stored using email capabilities.
14. All users must abide by the AUM Information Technology Appropriate Use Policy.

AUM Employees:

1. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and Hotmail etc. to conduct University business, to create or memorialize any binding transactions, or to store or retain email on behalf of AUM.
2. If AUM 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 within Outlook. If AUM employees receive confidential information via email or email attachments that is not required for University records, the information should be permanently deleted immediately. ITS can provide secured disk space for storing confidential information and will provide assistance upon request.
3. The originator of any AUM communications sent via email is responsible to determine and comply with the University Records Disposition Authority as to whether the materials need to be retained in another format or location. Additional information and assistance can be obtained from the University State Records Commission Liaison.
4. No confidential AUM data may be transmitted via email unless it has been rendered secure from unauthorized access. Upon request, ITS will provide assistance in securing confidential data.
5. Employees are prohibited from automatically forwarding AUM emails to a third-party email system. Individual messages that are forwarded by the user must not contain AUM confidential or sensitive information.
6. If an employee ends his/her employment with the University, AUM will disable access for the employee to his or her former email account. This process applies even if the employee is a former student at AUM. Employees who are currently taking classing at AUM and end their employment may retain access to their emails. In some cases, when it is in the best interest to the University, the

department in combination with the appropriate Dean or Vice Chancellor and the CIO may allow former employees to maintain access to their emails for a finite period of time.

7. If an employee retires, he or she may not retain access to his or her AUM employee email account. The retiree will be assigned a new email mailbox that is affiliated with AUM but separate from the employee email account. In some cases, when it is in the best interest to the University, the department in combination with the appropriate Dean or Vice Chancellor and the CIO may allow retirees to maintain access to their emails for a finite period of time.
8. While incidental personal use of email is acceptable, conducting business for profit using University resources is forbidden.

AUM Students:

1. Student email accounts will remain in effect for as long as the student remains enrolled in the University. The student may retain his/her email account upon graduation for 1 year.
2. Graduates who join the AUM Alumni Association may retain email access for the duration of their membership.
3. Student email accounts will be disabled immediately upon account holder being expelled from AUM for any reason or declared inactive for three consecutive semesters by the Registrar.

## VIII. SANCTIONS

Email accounts that are used in ways that violate this policy may be suspended. Deliberate disregard of this policy or the protection standards created to implement this policy may be subject to disciplinary action, in accordance with University policies and procedures, and FERPA regulations.

## IX. EXCLUSIONS

NONE

## X. INTERPRETATION

The Office of Technology CIO has the authority to interpret this policy.

**APPROVAL TO PROCEED:** ____________ **DATE:** 12-1-17

## APPENDICES

NONE