THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

ELECTRONIC MAIL AND OTHER ELECTRONIC COMMUNICATIONS

Number 06.01.06

Division Finance and Administration - Office of Information Technology (OIT)

Date June 2018

Purpose The purpose of this policy is to ensure the proper use of official university electronic mail (e-mail) and other electronic communications systems by its students, faculty, staff, and affiliates granted access to university electronic communication privileges.

Policy This policy establishes the principles and rules for the proper use of UAH official e-mail and other electronic communication systems. Electronic communication is a tool provided by the university to complement traditional methods of communications and to improve education and administrative efficiency. Users are responsible for using this resource in an efficient, effective, ethical, and lawful manner, and with normal standards of professional and personal courtesy. University e-mail and other electronic communications should only be used for official university business.

Use of the university's electronic communication systems evidences the user's agreement to be bound by this policy. This policy applies to all IT usage by faculty, staff, students, researchers, or other users of information technology (IT) e-mail or other electronic communications.

Procedure

1.0 Account Eligibility and Creation

Official e-mail addresses will follow a standard naming convention: 'ChargerID@uah.edu'

1.1 ChargerID

E-mail accounts for faculty, staff, and students are created based on the official ChargerID as reflected in Human Resources, Payroll, and Registrar

records. E-mail accounts for contractors or long-term visitors are based on the official name of the individual as reflected in the official request submitted by the campus sponsor, and will follow a similar naming convention as the official ChargerIDs for faculty, staff, and students. Requests for official ChargerIDs or affiliate accounts based on name preference, middle name, nicknames, etc., cannot be accommodated. ChargerIDs will remain in the system and will not be reused at any time.

1.2 E-mail Aliases

Requests for e-mail aliases may be submitted for approval through the OIT User Services portal website. The alias should be in the form of 'firstname.lastname@uah.edu'. Other forms of vanity e-mail aliases may be considered, but only in exceptional circumstances. E-mail aliases will only take effect after the request has been reviewed and approved.

1.3 Affiliate Accounts

Full-time faculty or staff may request temporary e-mail privileges for users outside of the university. The following will be required to submit user information, rationale for the account, a desired expiration date, and sponsor information. Affiliate accounts will be subject to review and expiration, but may be renewed by sponsor when appropriate.

1.4 Entity Accounts

Full-time employees of the university may request shared entity accounts which pertain to, or are reasonably related to, an individual or group's activities associated with the university. Such accounts would require designation of a university employee as the account owner, who will administer the account in accordance with these guidelines. Entity accounts will be audited on an annual basis.

1.5 Discussion Lists and Forum Accounts

Requests for a distribution group that functions as a forum or discussion list which pertain to, or are reasonably related to, an individual or group's activities associated with the university, may be accommodated. Such accounts would require designation of a group manager, who will administer the addition, deletion, or modification of names within the account, as well as manage the account in accordance with these guidelines. The request for such a group must originate with an active employee and is subject to approval. These accounts will be subject to review and expiration, but may be renewed by sponsor when appropriate.

Distribution groups will be able to receive mail from anywhere on the Internet, but will have no direct reply capability. The group/organization utilizing this type of group account will have to utilize their own personal mail account to respond to the originators of any mail received unless they wish to respond to the entire distribution list. These accounts will only be granted for Faculty/Staff recognized activities or organizations or Student Government Association (SGA) with approval of the faculty advisor being required for an organization recognized by the SGA.

2.0 Account Termination

See the “Network, Computer, and E-Mail Account Administration” policy for account expiration and termination governance.

3.0 Privacy of Electronic Communications

E-mail shall not be provided to anyone other than the account holder without approval from the data owner. In cases where the account holder is not available, but still affiliated with UAH, approval may be obtained by an official request from a senior executive officer of the university or Office of Counsel. If the account holder is no longer affiliated with UAH, the Director or unit head over that position may approve access.

Under certain circumstances, it may be necessary for the OIT staff or other appropriate university officials to access e-mail files to investigate security or abuse incidents or to investigate violations of this or other university policies. Access to email accounts will be granted on an as needed basis for these purposes and will follow pertinent law, policies, and regulations. Any e-mail accessed will only be disclosed to those individuals with a need to know, as determined in consultation with the Office of Counsel, or as required by law. E-mail account holders should have no expectation of privacy in connection with use of UAH E-mail systems and/or accounts.

E-mail is also subject to disclosure in response to regulatory investigations, court orders and lawfully issued subpoenas, and incident to the university's legal obligations to make certain information available to an opposing party during the legal process of discovery that precedes a trial. University employees must comply with university requests for copies of and/or access to e-mail records in their possession that pertain to the administrative business of the university or the disclosure of which is required to comply with applicable laws or other legal obligations of the university.

4.0 Acceptable Use of Electronic Communications

The university provides e-mail facilities for electronic communications that support the university's mission. All use of e-mail will be consistent with other university policies, and local, state, and federal law, including the Family Educational Rights and Privacy Act of 1974 (FERPA). When using e-mail as an official means of communication, faculty, staff, students, and affiliates should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, faculty, staff, students, or affiliates should not communicate anything via electronic communications they would not be prepared to say publicly. Faculty, staff, and students may not disclose personal, sensitive, or confidential university information in electronic communications that they are privileged to access because of their position at the university.

While reasonable personal use of electronic communications is acceptable, conducting business for profit using university resources, such as official e-mail, outside the purview of existing university policies related to the professional service and allowable consultancy components of the Faculty Handbook, is prohibited. Personal use of electronic communications must not be excessive and must not distract from or delay performance of university responsibilities of the user.

4.1 Examples of Inappropriate Use

Any inappropriate e-mail, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such e-mail should immediately contact OIT.

- The creation and/or exchange/forwarding of messages which are harassing, obscene, discriminatory, or threatening.
- The unauthorized exchange of proprietary information or any other privileged, confidential, or sensitive information.
- The creation and exchange of solicitations, chain letters and other unofficial, unsolicited e-mail.
- The creation of advertisements for non-UAH purposes.
- The creation and exchange of information in violation of any state or federal laws, including copyright laws, or university policies.
- The knowing transmission of a message containing a computer virus.
- The misrepresentation of the identity of the sender of an e-mail.
- The use or attempt to use the accounts of others without their permission.

5.0 User Responsibility

All electronic communications regarding university matters sent from an administrative office, faculty, or staff member are considered to be an official notice. Faculty, staff, students, and affiliates are expected to read e-mail on a regular basis and manage their accounts appropriately. Faculty, staff, or students who choose to use another e-mail system are responsible for receiving university-wide broadcast messages and other business-related e-mail by checking the university's official e-mail system and website. An alternate method of checking university e-mail is to utilize the 'forwarding' feature in university's official e-mail system, which can be set to forward mail to a different e-mail account. Note that when forwarding e-mail federal regulations such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and other regulatory requirements must be followed.

Sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All e-mail 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 these guidelines.

6.0 E-mail Retention and Backup

To the extent that they use e-mail messages as a substitute for a paper document; individuals are responsible for preserving those e-mail messages in accordance with any applicable federal, state, university or departmental records retention policies pertaining to the paper document for which the e-mail message is a substitute.

The Alabama State Records Commission has established a records disposition authority that outlines the required retention of records at public universities of Alabama. It is available at http://www.archives.state.al.us/officials/rdas/universityrda2.html.

Because of finite resources, the university has the right to restrict as necessary the amount of user space on e-mail servers provided by it, to revise retention policies with advance notice, and to purge and remove e-mail accounts in accordance with Section 2.0 Account Termination.

Official e-mail systems are backed up on a regular basis to allow recovery from a systemic loss impacting the entire e-mail system. While in some

cases it may be possible to recover from the accidental deletion of e-mail by a user, this is generally not feasible. If an individual or department feels the need to perform additional backups of individual accounts, the individual/department shall be responsible for creating and maintaining such backups. E-mail stored on desktops, laptops, workstations, or mobile devices is the user's responsibility to back up.

7.0 E-mail Servers

OIT maintains the university's official e-mail system. Any entity desiring to operate an independent e-mail server does so at the discretion of OIT. If such operation is approved, the server must be registered and approved with OIT. E-mail delivery will be blocked to all non-registered systems.

The organization responsible must adhere to and be audited for compliance with security criteria established by OIT for university systems. This includes, but is not limited to, properly securing the e-mail servers and retaining a copy of all emails transmitted through the e-mail server for the period of one year for all university employee accounts.

8.0 Spam, Phishing, and Viruses

The Office of Information Technology may, at its discretion, choose to scan incoming and outgoing electronic communications for viruses, phishing attempts, and/or spam. Messages determined to be malicious may be blocked to reduce risk to the university.

The university's official e-mail system allows for individuals to configure spam and phishing scanning settings for their account.

Legitimate representatives of the university will never require you to send account access details, such as user IDs and passwords, to them via e-mail. Any message requesting such information should be considered phishing and should be reported to the Helpdesk and discarded, without response.

9.0 Compliance with Policy

OIT personnel may take immediate action to abate identified issues impacting network or system operations.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, the Staff Handbook, or University policy, will be referred to appropriate university authorities.

Review The IT Investment Advisory Council is responsible for the review of this policy every five years (or whenever circumstances require).