Augusta University / Augusta University Health

Acceptable Use of Electronic Mail & Electronic Messaging Policy

Policy Owner: Chief Information Security Officer

SCOPE

This policy establishes standards for the acceptable use of electronic messaging and applies to electronic mail (email), instant messaging, and any other messaging technology as defined in the policy. Augusta University utilizes the augusta.edu domain for its email platform, and this is the single official university email system.

POLICY STATEMENT

I. Purpose of Electronic Mail & Electronic Messaging

Augusta University (AU) provides electronic messaging and email services on behalf of itself and AU Health System, Inc. (AUHS), to include its affiliates. No employee shall use an email or messaging service for official/work related communication other than that provided by AU, unless they have received advance written permission from the Vice President for Information Technology/Chief Information Officer. Electronic messaging and email are provided to support the educational, research, service, and administrative activities of the university and health system, and serve as an official means of communication by and between users of the AU community and its constituents. The purpose of this policy is to ensure this critical service remains highly available, reliable and supports purposes appropriate to AU's mission.

Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of an AU email account evidences the user's agreement to be bound by this policy.

II. Ownership of Electronic Data

AU owns all AU email accounts. Subject to underlying copyright and other intellectual property rights under applicable laws and AU policies, AU also owns data created, transmitted, and/or stored using the AU email accounts.

III. Acceptable Use of AU Provided Email and Electronic Messaging Accounts

Email users have a responsibility to learn about and comply with AU's acceptable uses of email and electronic messaging services. Violation of AU's policies may result in disciplinary action dependent upon the nature of the violation.

Originally Approved: September 28, 2018

Examples of acceptable use:

- Dissemination of mission related information to other members of the AU community (students, faculty, staff, alumni, etc.)
- Transitory correspondence to support the mission of the university and health system.

Examples of **prohibited** uses of email include but are not limited to:

- Unauthorized use of a commercial or private email service for work related purposes;
- Unauthorized access to other's email or messaging accounts, including those assigned to other individuals and system accounts;
- Intentionally distributing spam, phishing, chain letters, or any other type of unauthorized widespread distribution of unsolicited email;
- Use of email for commercial activities, personal gain, or political activities including partisan political or lobbying activities;
- Representing yourself as another individual or organization to send communications;
- Use of email to transmit materials in a manner which violates any laws including but not limited to intellectual property and copyright laws;
- Generating or facilitating unsolicited bulk email;
- Messaging that infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- Use of email for any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- Interferes with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized users;
- Alters, disables, interferes with or circumvents any aspect of the email services;
- Tests or reverse-engineers the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
- Constitutes, fosters, or promotes pornography;
- Is excessively violent, incites violence, threatens violence, or contains harassing content;

- Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Misrepresents the identity of the sender of an email.

Other improper uses of the email system include but are not limited to:

- Using or attempting to use the accounts of others without their permission;
- Collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting);
- Use of the service to distribute software that covertly gathers or transmits information about an individual;
- Conducting business for profit under the aegis of AU.

The foregoing list is not intended to be exhaustive but rather to provide illustrative examples.

IV. Expectation of Privacy & Right of University Access

AU will make reasonable attempts to keep email messages secure; however, users should have no general expectation of privacy in email messages sent through AU provided email or messaging accounts.

Under certain circumstances, it may be necessary for AU officials to access various email accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security, privacy, or abuse, and/or investigating violations of this or other AU policies, violations of the email Provider's Acceptable Use Policy, or AU contracts with the email provider.

AU staff or officials may also require access to an AU email account in order to continue AU business where the University Email Account holder will not, or can no longer, access the university email account for any reason, e.g., death, disability, illness, permanent or temporary separation. Such access will be on an as-needed basis, and any email accessed will only be disclosed to individuals who have been properly authorized and have an appropriate need to know, or as required by law.

V. Data Purging & Email Archiving

Individuals are responsible for saving email messages as appropriate. Unless a legal hold has been placed on an account, messages in AU's email accounts are automatically and permanently archived and purged from the active "in-box" and email folder structures as follows:

- Sent / Sent Items - 60 days
- Trash / Deleted Items - 15 days
- Junk / Junk Email - 30 days
- Inbox and Other Folders Not Specified Above – 180 days

AU provides a secure email archiving solution for users to access emails that are automatically purged after 180 days.

Due to finite resources, AU reserves the right to restrict the amount of user space on AU provided email accounts, and the size of email archives. Individuals should not rely on an email account to archive data and each person is responsible for saving individual messages and attachments as appropriate.

VI. Sensitive Information

Sensitive and confidential data should only be transmitted through secure methods. AU provides tools for this purpose and employees have a responsibility to familiarize themselves with the use of these tools.

Sensitive information should not be created, transmitted, or stored on any AU email or messaging system **unless it has been explicitly approved by policy and encrypted at all times**. Sensitive information includes, but is not limited to, any information relating to identified or identifiable individual or entity that is confidential, proprietary, or sensitive to such individual or entity and may cause harm to such individual or entity if accessed, used, or disclosed by unauthorized persons, or lost, either internal or external to AU or AU Health. Sensitive information also includes, but is not limited to, confidential information, Protected Health Information (PHI), Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Social Security number, bank account information, tax forms, background checks, sensitive research data, audit reports, and other information subject to applicable federal and state law.

VII. Required Security Measures for all Electronic Messages containing PHI or PII

Unencrypted messages containing PII or PHI may not be sent utilizing AU's email system for any reason.

Encrypted PII or PHI may be sent via AU's official email system only when AU and AU Health personnel fully comply with the following security measures:

1. Electronic messages containing PHI may not be sent or received except with a device that has been secured in compliance with AU's security policies and procedures.
2. PII or PHI must be limited to the minimum information necessary.
3. Highly sensitive PHI (for example, mental health, substance abuse, or HIV information) should only in exceptional circumstances be transmitted by email, and must be encrypted.
4. AU personnel must use their official AU email account to send and receive properly encrypted PII or PHI, and they may not use any other email accounts (for example, Google or Yahoo accounts) for that purpose.
5. PII or PHI may only be sent by encrypted email after the recipient's address has been carefully verified (for example, from a directory or a previous email) and entered correctly.
6. PHI may never be sent through an instant messaging program unless specifically authorized by the Chief Information Security Officer.

VIII. Expiration of Accounts

Individuals may leave AU for a variety of reasons, which gives rise to differing situations regarding the length of email privileges or expiration of accounts. The policy governing those privileges are set forth below. Notwithstanding the guidelines below, AU reserves the right to revoke email privileges at any time.

- **Faculty who leave before retirement** – Faculty who leave before retirement may keep their email account for one year from the end of the last term in which they taught. If such separation is for cause, email privileges may be immediately revoked without notice.
- **Staff who leave before retirement** – Staff who leave the university will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice.
- **Retired Faculty** – Faculty who have retired from the university will be permitted to retain their email privileges if their account remains active. All email accounts that are inactive for a period of one year will be removed.
- **Retired Staff** – Staff who have retired from the university will have email privileges removed effective on their last worked day.
- **Students who leave before graduation** – Students who leave the university without completion of their degree or other program may keep their email privileges for one academic year from the last term when they were registered.
- **Expelled students** - If a student is expelled from the university, email privileges will be terminated immediately upon the directive of the Dean of Students Office.

- **Alumni** – Students who have graduated from the university will be permitted to retain their email privileges if their account remains active. All email accounts that are inactive for a period of one year will be removed. Alumni wishing to reconnect with the university can request an account and one may be provided.

IX. Sharing of Passwords

In order to prevent the unauthorized use of email accounts, the 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 assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

X. Email Forwarding

An AU email account may never be set to auto-forward messages to a non-AU account.

XI. Exceptions

Exceptions to this policy may be granted for operational reasons or to comply with law, regulation, or guidance from regulatory authorities. All exceptions will be reviewed on a period basis.

DEFINITIONS

Protected Health Information: PHI as defined in the Health Insurance Portability and Accountability Act of 1996 privacy regulations, ("HIPAA"), as amended.

Sensitive Information: any information relating to identified or identifiable individual or entity that is confidential, proprietary, or sensitive to such individual or entity and may cause harm to such individual or entity if accessed, used, or disclosed by unauthorized persons, or lost, either internal or external to AU or AU Health. This includes, but is not limited to Confidential Information, Protected Health Information, Personally Identifiable Information, Payment Card Industry (PCI) data, undisclosed financial statements, audit reports, and other information subject to applicable federal and state law.

Employee/Augusta University Workforce: full-time or part-time employees, trainees, vendors, contractors, or any other individuals who may create, use, disclose, access, or transmit any sensitive information.

An **Electronic Message** is any message created, sent, forwarded, replied to, transmitted, stored, copied, downloaded, displayed, viewed, or read by means of telecommunications networks or computer systems. This definition applies equally to

the contents of such messages; transactional information associated with such messages, such as headers, summaries, addresses, and addressees; and attachments (text, audio, video). This Policy applies only to Electronic Messages in their electronic form. The Policy does not apply to printed copies of Electronic Messages.

An **Electronic Messaging System** is any messaging system that depends on electronic facilities to create, send, forward, reply to, transmit, store, copy, download, display, view, or read Electronic Messages, including services such as email, text messaging, instant messaging, social networking, blogging, electronic bulletin boards, listservs, and newsgroups.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning to the data without the use of a confidential process or key.

SPAM is defined as unsolicited and undesired advertisements for products or services sent to a large distribution of users.

Phishing is defined as the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: October 17, 2018

President, Augusta University and CEO, AU Health System
Date: October 25, 2018