# Augusta University
# Policy Library

# Acceptable Use of Electronic Mail & Electronic Messaging Policy

### Policy Manager: Chief Information Security Officer

**POLICY STATEMENT**
Augusta University (AU), hereinafter referred to collectively as "AU", provides electronic mail services to faculty, staff, students, and to other affiliated classes of individuals, including alumni and to others in the AU community for official approved purposes. It is a goal in this policy for AU to provide guidance in meeting the fundamental requirements for electronic mail and electronic messaging to ensure data security, data privacy, effective use and compliance with relevant laws and policies. AU is committed to protecting Family Educational Rights and Privacy Act (FERPA), Payment Card Industry (PCI), electronic Protected Health Information (ePHI) data, and/or other sensitive information (SEI) by implementing physical security standards within facilities and within areas of a facility that contain or provide access to FERPA, SEI, PCI or ePHI data.

This policy is in accordance with requirements of the University System of Georgia (USG), USG IT Handbook - Section 5.15 Email Use and Protection.

It is the policy of AU to provide guidance for the acceptable use of electronic messaging and this policy applies to electronic mail (email), instant messaging, and any other messaging technology as defined in the policy. It is AU's intent to protect the confidentiality of our students, patients, faculty, and staff, and to reduce adverse impacts to the University. AU will use best practices and industry standards to protect FERPA, ePHI, PCI data (and other confidential and proprietary electronic information) and to provide guidance for the use of electronic messaging using approaches that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that federal, state, or local laws and regulations are followed.

This policy addresses USG requirements for adhering to the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations (as well as changes made through the Health Information Technology of Economic and Clinical Health Act (HITECH)) and other applicable federal, state, or local laws and regulations that may relate to the protection and security of SEI.

AU shall encrypt all sensitive information in alignment with relevant National Institute of Standards and Technology (NIST) standards Cybersecurity Framework (CSF) and best practices for sensitive email both in transit and at rest. Business systems managers of any system(s) used for electronic messaging within or utilized by the AU that cannot be encrypted due to technical limitations shall submit a waiver to the Chief Information Security Officer (CISO). The CISO may grant waivers to this policy providing compensating controls are documented.

---

**Office of Legal Affairs Use Only**
**Executive Sponsor: VP for Information Technology**
**Next Review: 5/2027**

**AFFECTED STAKEHOLDERS**
*Indicate all entities and persons within the Enterprise that are affected by this policy:*

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☒ Visitors
☒ Other: All members of the AU community who are entitled or permitted to have electronic mail or electronic messaging services.

**DEFINITIONS**

1. **AU Community**: full-time or part-time employees, trainees, vendors, contractors, alumni, non-paid affiliates, faculty, emeritus faculty or any other individuals who may create, use, disclose, access, or transmit any sensitive information.

2. 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.

3. 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.

4. **Electronic Protected Health Information (ePHI):** ePHI as defined in the Health Insurance Portability and Accountability Act of 1996, ("HIPAA"), as amended. *ePHI* means individually identifiable health information that is Transmitted by electronic media or Maintained in electronic media

5. **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.

6. **Family Educational Rights and Privacy Act of 1974 (FERPA)**: (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education**.**

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

8. **Payment Card Industry Data Security Standard (PCI DSS):** Data collected by organizations that accept, store, transmit, or process cardholder data must comply with the PCI DSS and is administered by the PCI SSC (Payment Card Industry Security Standards Council) to decrease payment card data security. This includes sensitive data that is presented on a card or stored on a card – and personal identification numbers entered by the cardholder.

9. **Personally Identifiable Information (PII)**: any information that permits the identity of an individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

10. **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. 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.

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

12. **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.

## PROCESS & PROCEDURES

1. **Purpose of Electronic Mail & Electronic Messaging.** AU provides electronic messaging and email services to its active students, employees, emeriti faculty, affiliates with documented business need. 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.

2. **Ownership of Electronic Data.** AU owns all AU email accounts and the contents within. 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. **AU's email is not an official system of record, and therefore is not subject to retention under Georgia Archives Policy.**

3. **Email Provisioning.**

    a. **Student Accounts** are granted to all registered students of AU prior to their first semester and are retained for the duration of the student's active relationship with the University. Students may access their email accounts once they have been issued their Jag ID, received from Admissions upon acceptance to the University.

    b. **Faculty & Staff Email Accounts** are requested by Human Resources to IT helpdesk. IT creates the account, and the information is provided to the requestor. These accounts will remain with the individual until employment status with AU terminates or changes.

    c. **Non-paid Affiliate Email Accounts** will not automatically be provided email services. Should a department request an account for a non-paid affiliate, the department will need to bear the annual costs for as long as that account remains active. Departments are required to notify IT immediately when the business requirement for the non-paid affiliate ends.

| Email Account Type | Provisioning |
|---|---|
| Student | Prior to first Semester |
| Faculty | During onboarding process |
| Staff | During onboarding process |
| Non-paid Affiliate | Created by business justifications and organizational business needs |

4. **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 is set forth below. Notwithstanding these guidelines, AU reserves the right to revoke email privileges at any time. No individual will be authorized to retain any regulated or sensitive data upon departure without consultation with the AU Privacy Office and the expressed written approval from the AU Legal Office. If this information cannot be purged from the account, then continued access to the account will not be granted.

    a. **Student Email Account Termination Practices**
        I. Students are inactivated in multiple ways by the University, at which time their email accounts will be inactivated:
            (a) No Show process – students who did not complete their enrollment during admissions processes

(b) Graduation – students are inactivated after graduation is processed
(c) No attendance – students who are not enrolled in classes for 3 consecutive semesters
(d) Inactive medicine residents – manually inactivated when the Graduate Medical Education office notifies the Registrar's office they will not attend.

II. Student email privileges will be revoked if a student is expelled from the university, email privileges will be terminated immediately upon the directive of the Dean of Students Office.

b. **Faculty, Staff, & Non-Paid Affiliate Email Account Termination Practices.**

I. Upon end of employment (retirement, resignation, for cause termination), employee email **access** ends immediately, when the termination is processed in OneUSG (typically the day following the last day of employment). AU leadership may determine an individual's access be removed immediately. Account will be inactivated 30 days after termination, and all historical email data will be permanently deleted.

II. Emeritus faculty will be allowed to maintain their AU email account. However, after official termination, the contents of the email account will be deleted in order to ensure the confidentiality of any sensitive information within the account.

III. President or EVP has discretion to determine if there is an "official need" for ex-employee to support AU through email access, for **limited** period. The requesting department will be responsible for paying for this additional access.

IV. Thirty days after termination, all historical email data will be permanently deleted unless the account is under litigation hold.

V. Litigation hold can be activated on those accounts identified by Legal to retain emails as necessary.

VI. Inactive account information can be transferred to successor employee if there is a business need and the request is made within 30 calendar days of the employee's termination. Any longer than 30 days, access can no longer be transferred.

VII. If a college or department would like to have an employee maintain access after their termination date, the request must be made within 30 days of the employee's termination and be approved by the President or EVP. The account will be converted to a non-paid affiliate and the department would bear the annual cost for as long as the account remains active.

VIII. When an employee is terminated on one platform, and rehired on another platform, they may be issued a new account and will no longer have access to their historical data from their former employment role.

IX. All faculty and staff are required to participate in off-board training, provided by Human Resources, to ensure options associated with their accounts and data are understood.

| Email Account Type | Expiration |
|---|---|
| Student | Termination of student's active relationship with AU |
| Faculty | Termination of Faculty's active relationship with AU |
| Staff | Termination of active relationship with AU |
| Non-paid Affiliate | Termination of account will occur when they are not renewed, or business relationships are no longer essential |

5. **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. The following list is not intended to be exhaustive but rather to provide illustrative examples.

    a. Users of AU provided electronic mail and messaging services, will not share their access credentials, and will abide by the Password Protection and Acceptable Use of Information Technology policies when using these resources.

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

    c. Examples of acceptable use:
        I. Dissemination of mission related information to other members of the AU community (students, faculty, staff, alumni, etc.)
        II. Transitory correspondence to support the mission of the university and health system.

    d. Examples of **prohibited** uses of email include but are not limited to:
        I. Unauthorized use of a commercial or private email service for work related purposes;
        II. Unauthorized access to other's email or messaging accounts, including those assigned to other individuals and system accounts;
        III. Intentionally distributing spam, phishing, chain letters, or any other type of unauthorized widespread distribution of unsolicited email;
        IV. Use of email for commercial activities, personal gain, or political activities including partisan political or lobbying activities;
        V. Representing yourself as another individual or organization to send communications;
        VI. Use of email to transmit materials in a manner which violates any laws including but not limited to intellectual property and copyright laws;
        VII. Generating or facilitating unsolicited bulk email;

VIII. 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;
IX. Use of email for any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;
X. Intentionally distributing viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
XI. Interfering with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized users;
XII. Altering, disabling, interfering with, or circumventing any aspect of the email services;
XIII. Testing or reverse-engineering the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
XIV. Constituting, fostering, or promoting pornography;
XV. Using language that is excessively violent, incites violence, threatens violence, or contains harassing content;
XVI. Creating a risk to a person's safety or health, creating a risk to public safety or health, compromising national security, or interfering with an Investigation by law enforcement;
XVII. Improperly exposing trade secrets or other confidential or proprietary information; misrepresenting the identity of the sender of an email; purposefully trying to circumvent any technical control.

e. Other **improper uses** of the email system include but are not limited to:
I. Using or attempting to use accounts other than approved for delegated access;
II. 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);
III. Using the service to distribute software that covertly gathers or transmits information about an individual;
IV. Conducting business for profit under the aegis of AU.

6. **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. Emails and messaging may be subject to submission under the Georgia Open Records Act or other federal laws.

a. 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.

b. 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.

7. **Email Archiving**. AU provides a secure email archiving solution for users with active accounts to access emails that are automatically archived 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. Email is not considered an appropriate data storage location. Any data critical to work activities should be moved from email messages and into an appropriate approved system of record.

8. **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 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. 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.

9. **Required Security Measures for all Electronic Messages containing PHI or PII.** Unencrypted messages containing regulated data may not be sent utilizing AU's email system for any reason.

    a. Any person sending email containing sensitive or protected information must secure the message by inserting the word '**secure'** in the subject line of the email.
        I. The word '**secure**' is not case sensitive.
        II. The word '**secure'** can be anywhere in the subject line.
        III. Remember to check that you are sending the email to the correct recipient before hitting Send.

    b. All emails containing sensitive or protected information must include the word '**secure**' in the subject line. This includes messages for internal or external recipients. Messages sent internally to other AU recipients will not look different because they are already secured within our email system. In the event

a message gets forwarded to someone outside of AU, the message already containing the '**secure**' tag in the subject line, will then be secured through current AU security control systems.

c. Encrypted PII or PHI may be sent via AU's official email system only when AU personnel fully comply with the following security measures:
    I. 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.
    II. PII or PHI must be limited to the minimum information necessary.
    III. 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.
    IV. 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.
    V. 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.
    VI. PHI may never be sent through an instant messaging program unless specifically authorized and when done so with an approved application.
    VII. AU email communication should only be conducted using AU provided email, personal accounts are not acceptable communication for AU business.

10. **Reporting**. When suspected malicious emails or phishing is suspected, it then becomes the individual's responsibility to report this to AUHS's Cybersecurity department for investigation. See *Cyber Security Incident Response Policy.*

    a. Cybersecurity Incident Hotline: 706-722-CYBER (9237)
    b. IT Service Desk: 706-721-4000
    c. Forward suspected malicious emails to: 72Cyber@augusta.edu

11. **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 periodic basis or as needed.

**REFERENCES & SUPPORTING DOCUMENTS**
Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security regulations
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended
Payment Card Industry (PCI) PCI Security Standards Council
Privacy Rule (16 C.F.R. Part 313)
USG IT Handbook - Section 5.15 Email Use and Protection

**RELATED POLICIES**
Acceptable Use of Information Technology
Cybersecurity Training Policy
Data Management Classification
Electronic Access Control
Electronic Data Retention
Electronic Data Storage Backup
Encryption Policy
Password Protection Policy

**APPROVED BY:**

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/20/2022

President, Augusta University Date: 5/20/2022