Electronic Communication Policy

I. PURPOSE
The electronic communication services of Salem State University are vital to the support of the educational, administrative and public service activities of the University. The purpose of this policy is to ensure that these critical services remain available and reliable, and are used for purposes appropriate to the mission of Salem State University.

II. SCOPE
This policy applies to all users of any electronic communication service supported or used by the University.

III. POLICY
Salem State University authorizes the use of electronic communication services for official communication between students, staff, faculty, administrative users and the public. All members of the campus community are expected to comply with established guidelines and procedures which define the proper use of these services.

While the University will make reasonable efforts to maintain the integrity and effective operation of its electronic communication services, users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the University can assure neither the privacy of an individual user's use of the resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

IV. PERMISSIBLE USES OF ELECTRONIC COMMUNICATION SERVICES

1. Authorized Users: Only University faculty, staff, students, contractors and other members of the University community who have received permission under the appropriate University authority are authorized to use the University's electronic communication services. Individual accounts remain for the exclusive use of the individual for whom they were assigned, and cannot be shared; however authorized proxies are permitted.

2. Purpose of Use: The use of any University resource for electronic communication must be related to University business or academic pursuits. Incidental and occasional personal use of electronic communication services may occur when such use does not generate a direct cost for the University. In the event of such an incidental or occasional use, the provisions of this policy will still apply.

3. Message Archiving: Individuals are responsible for saving or archiving electronic messages that constitute official University records. Due to limited resources, the Office of Information and Technology Services has the right to restrict the amount of user space on a message server as necessary and to purge and remove electronic accounts of students who have not registered for a specified period of time.

4. Inspection and Disclosure of Communications: The University reserves the right to inspect and disclose the contents of electronic communications in the course of legally or ethically mandated investigations. Such investigations may be triggered by
indications of misconduct or misuse, as needed to protect health and safety, as needed to prevent interference with the academic mission, or as needed to locate substantive information required for University business that is not more readily available by some other means. The University will inspect and disclose the contents of electronic communications when such action is necessary to respond to legal processes and to fulfill the University's obligations to third parties.

5. Disclosure and Use of Information: The contents of electronic communications, properly obtained for University purposes, may be disclosed without permission of the user. The University will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

6. Special Procedures to Approve Access: Individuals needing to access the electronic communications of others, to use information gained from such access, and/or to disclose information from such access must have the prior consent of the user. In absence of such consent, they must obtain advanced approval of such activity from the appropriate University vice president, dean, or higher authority.

V. PROHIBITED USES OF ELECTRONIC COMMUNICATION SERVICES

Prohibited uses of the University’s electronic communication services include, but are not limited to the following:

1. Any personal use that creates a cost for the University, or interferes with a University employee’s obligation to carry out University duties in a timely and effective manner is prohibited.

2. No use is permitted for personal monetary gain or for any commercial purposes that are not directly related to University business.

3. Under no circumstance should sensitive Personally Identifiable Information (PII) such as names with social security number, financial account number, credit card number or driver's license number be transmitted from or requested by the university via eCommunications.

4. No use is permitted that conflicts with the requirements of civil or criminal law, including but not limited to laws relating to pornography, defamation, copyright, intellectual property infringement, and illegal discrimination, or conflicts with any applicable policy of the Board of Trustees, such as use in support of partisan political activities.

5. No transmission of FERPA protected data is permitted.

6. No use is permitted that constitutes the unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

7. The capture of any electronic messages, except as required by authorized employees operating within the guidelines of approved University-wide policies, is not permitted.

8. The use of electronic communications to harass or intimidate others is strictly prohibited.

9. The knowing transmission of a message containing a computer virus or that misrepresents the identity of the sender is prohibited.

10. The transmission of any message of excessive size or volume that interrupts or degrades the service to the University community is prohibited.
11. No personal use may state or imply University sponsorship or endorsement of its message.
12. Attempting unauthorized access to electronic communications or attempting to breach any security measures or policies on any electronic communication system, or attempting to intercept any electronic transmissions without proper authorization is prohibited.

VI. OFFICIAL UNIVERSITY ELECTRONIC COMMUNICATIONS

When using electronic services as an official means of communication, students, faculty and staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, they should not communicate anything electronically that they would not be authorized and prepared to say publicly.

Those wishing to transmit broadcast electronic messages containing essential University announcements to students, faculty, and/or staff must obtain approval from the appropriate administrative authority. Within the scope of their authority, only the offices of a Department Chairperson, Director, Dean, Vice President, or President may authorize the transmission of broadcast messages to an audience of more than 100 recipients. Every effort should be made to use established and approved mass distribution lists to selected University communities.

Appropriate broadcast of electronic messages may include, but is not limited to, the following types of announcements:

1. Emergency or unforeseen campus-wide events notification (e.g., cancellation of classes or closing of the University due to inclement weather or emergency).
2. Important campus deadline notifications (e.g., last day of drop/add for students).
3. Improved services to students, faculty or staff that directly impact all members of the affected group.

By contrast, broadcast electronic messages should not contain attachments and should only be used to promote the interests of the University. Broadcast email messages should be sent only to the affected group (students, faculty, or staff, or a subgroup of one of those groups) and should be of critical importance to that group.

VII. USER RESPONSIBILITIES

Faculty, staff, and students are expected to read their University electronic messages on a regular basis. Those who choose to use another email system are responsible for any redirection and for ensuring accurate receipt of such messages. An electronic message regarding University matters sent from an administrative office to the official email address of a faculty, student or staff member is considered to be an official notice from the University.

Email lists are provided as a service to faculty, staff and students for posting University-related information. These will be monitored by those responsible for their content; any posted material deemed inappropriate by University administrators based upon the standards set forth above may be removed without prior notification.

VIII. ENFORCEMENT

All members of the University community are bound by federal and local laws relating to civil rights, harassment, copyright, security and other statutes relating to electronic communications. This policy does not preclude enforcement under the laws and regulation
of the United States of America or the Commonwealth of Massachusetts.

The University reserves the right to monitor and record the usage of all electronic transmissions as necessary to evaluate and maintain system efficiency and acceptable use; and may further monitor, record or legally disclose usage by individuals, including the disclosure of individual file content.

IX. VIOLATION OF POLICY

Violation of this policy may subject a user to disciplinary action under appropriate University disciplinary procedures. The University may take such action as necessary, in its discretion, to address any violation(s) under this policy.

X. DISCLAIMER

The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic resources and communication are warned that they may come across or be recipients of material they find offensive.

XI. SUPPLEMENTAL REGULATIONS AND STANDARDS

Acceptable Use: Acceptable Use Policy for University services.

Executive Order 504: Massachusetts Executive Order regarding the security and confidentiality of personal information

Family Educational Rights and Privacy Act (FERPA): (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.


Identity Theft Law: Massachusetts law relative to security freezes and notification of data breaches (Chapter 82 of the Acts of 2007).