Use of Technology Policy

Policy Number	STU-025
Effective Date	December 17, 2007
Responsible Office/Person	CITS

Policy Statement
All members of the University community are required to comply with policies specifically pertaining to the use of campus technology.

Purpose
The University operates in a large, complex information-technology environment requiring communications related to both confidential and public data. New technologies offer the University methods to make this communication easier between students, staff, departments, campuses, colleges and the world. The University has several types of electronic mail systems on its various computer systems, enabling its students and employees to take advantage of these technologies.

However, with this open communication network, vulnerabilities to the privacy of electronic messages possibly containing confidential or proprietary material arise. University electronic mail users need to be aware of the vulnerabilities in electronic mail communication and of legal responsibilities that accompany the use of this medium.

Definitions
These standards:

Define who may use the electronic mail systems controlled and administered by the University of Massachusetts (the University),
Outline responsibilities related to electronic mail maintenance and use,
Provide guidelines for the security and confidentially of University electronic mail, and
Provide methods for monitoring, enforcing and dealing with exceptions to this policy.
Campus Electronic Mail Policies shall apply to all:

Electronic mail (e-mail) created, sent or maintained within, administered by or networked to the electronic mail systems of the University of Massachusetts.
University e-mail users.

Electronic mail as defined in the Definitions Addendum to this standards document.
Responsibilities

The President, together with the Chancellors of all UMass campuses, will define what categories of individuals (e.g., full time, part-time, staff, students, economic partners, other educational institutions, general public, etc.) may access University electronic mail systems. The Chancellors will determine:

Which University department(s) shall be responsible for administering electronic mail systems and security.
Procedures for electronic mail monitoring related to Section IV, Item E of this standards document.
Campus Electronic Mail Policies will ensure that Electronic Mail Administrators are responsible for:

Determining what categories of individuals, within the guidelines set by the President and campus Administrators, may access the mail system under their control.
Ensuring that a security plan for which they are responsible, has been developed, implemented and is maintained. The security plan should include an analysis of whether message encryption is needed.

Ensuring that a backup plan to allow for message/system recovery in the event of a disaster has been developed, tested and implemented.
Ensuring that deleted and expired mail is not backed up for more than 30 days. After 30 days deleted and expired messages will be unretrievable for reasons of resource utilization and liability. This standard applies to deleted mail only. If does not apply to mail in users mailbox or electronic mail file folders.
Periodically assessing the level of risk within the mail system.
Ensuring that filters to keep text from view of system maintenance personnel have been installed, when technologically possible.
Ensuring that appropriate steps are taken to prevent a system break-in or intrusion through the electronic mail application.
Providing information regarding electronic mail vulnerabilities to e-mail users so that they may make informed decisions regarding how to use the system.
Ensuring that all electronic mail ID's for individuals with email accounts in University systems have been deleted when: an authorized user has terminated employment, graduated or withdrawn from the University, and when a "courtesy account" is inactive or no longer needed.

Ensuring that e-mail message retention standards, within the guidelines of these and other University policies, have been developed and are implemented for their electronic mail system.
Campus Electronic Mail Policies will ensure that employees responsible for maintaining, repairing and developing email resources will exercise special care and access email messages

only as required to perform their job function. These employees will not discuss or divulge the contents of individual email messages viewed during maintenance and troubleshooting.
Campus Electronic Mail Policies will ensure that University Email Users will:

Use email in a responsible manner consistent with other business communications (e.g., phone, correspondence).
Safeguard the integrity, accuracy and confidentially of University electronic mail.
Only use mail IDs assigned to them.
Remove mail from their mailbox consistent with University, campus departmental or electronic mail administrator message retention policies and standards.
Campus Electronic Mail Policies will ensure that University email users will NOT:

Send any unsolicited mail or materials that are of a fraudulent, defamatory, harassing, or threatening nature.
Post materials that violate existing laws or University codes of conduct, are inconsistent with the University mission, or are commercial advertisements or announcements on any electronic bulletin boards.
Forward any other form of unnecessary mass mailing (such as chain letters) to University or external email users.
Use their email access to unlawfully solicit or exchange copies of copyrighted software.
Electronic Mail Security and Confidentiality Standards

Campus Electronic Mail Policies will ensure threat email users are aware and understand that:

The University considers an email message as a personal or business correspondence which should therefore, be dealt with in the same manner.

The University considers electronic mail messages the property of the sender and/or receiver. Although the messages are considered the property if the sender and/or receiver these messages are stored on the University computer systems and the University is therefore, responsible for the administration of electronic mail.
The right to privacy is not inherent on an electronic mail system, especially one connected to the Internet.
The University will not monitor the content of electronic documents, or however, the privacy of documents and messages stored in electronic media cannot be guaranteed. Electronic documents and messages may be readable to maintenance, security and troubleshooting staff while performing their job functions. Such access occurs only when a problem in the software or network arises. Additionally electronic mail may pass out of one computer environment, across a network, and into another totally different computer environment even within the University system, This transport becomes increasingly complicated as mail travels between departments, campuses, universities, states, or nations. The level of security over your message is affected each time the computer hardware, software and environment changes.

Untraceable leaks may occur.
If there is a University investigation for alleged misconduct, the Chancellor or their designee may authorize that electronic mail or files may be locked or copied to prevent destruction and loss of information. Additionally, the University may monitor the content of electronic documents and messages, or access email backups or archives as a result of legal discovery, writ, warrant, subpoena, or when there is a threat to the computer systems integrity or security.

The confidentiality of the contents of email messages that include certain types of information (e.g., student related, medical, personal) may be protected by the Family Educational Rights and Privacy Act of 1974 (as amended) and/or the Electronic Communications Privacy Act of 1986. Additionally the contents of email messages may be classified as public by the Massachusetts Fair Information Practices Act (M.G.L. c66A) and/or the Massachusetts Public Records Act (M.G.L. c66).

The authenticity of an email message cannot be assured due to the state of present email technology. This means that t the authorship or source of an email message may not be as indicated in the message.

University Email Users may retain active mail files for the retention period by the Electronic Main Administrator. Deleted and expired email messages will e unretrievable after 30 days.
Electronic Mail Use Standards

Policies will adhere to the following standards:

Individuals are prohibited from using an electronic mail account assigned to another individual to either send or receive messages. If it is necessary to read another individual's mail (e.g., while they are on vacation, on leave, etc.) surrogacy or message forwarding should be requested from the email administrator.
University E-Mail Users are encouraged to use these communications resources to share knowledge and information in furtherance of the University's missions of instruction, research, and public service. Occasional and incidental social communications using electronic mail are not prohibited; however such messages should be limited and not interfere with an employee's job function.

Individuals with email ids on University computer systems are prohibited from sending messages which: violate existing laws, or University code of conduct or policies; are inconsistent with the University mission; or are advertisements or announcements for a commercial business.

Authorized users should not: rebroadcast" information about significant issues obtained from

another individual that the individuals reasonable expected to be confidential.

Bulletin Boards used for soliciting or exchanging copies of copyrighted software not permitted on University electronic mail systems.

Authorized users are prohibited from sending, posting or, publicly displaying or printing unsolicited mail or materials that is of a fraudulent, defamatory, harassing, abusive, obscene or threatening nature on any University system. The sending of such messages/materials will be handled according to current University codes of conduct, policies and procedures.

The University accepts no responsibility for the content of electronic mail received. If a student receives electronic mail that they consider harassing, threatening or offensive, they should contact the appropriate University Office for assistance.

Remember, federal and state laws, and University policies against racism and sexual harassment exist. Additionally, the University has special concern for incidents in which individuals are subject to harassment or threat because of membership in a particular racial, religious, gender or sexual orientation group.

Procedures
Campus Electronic Mail Policies should ensure that any individual found breaching the confidentiality of email messages, disclosing confidential University data, or otherwise violating this policy may be denied future access to the computer system and shall be subject to reprimand, suspension, dismissal, or other disciplinary actions by the President or his/her designee consistent with University delegations of authority, the Student Code of Conduct, personnel policies, and union agreements.

Responsibility
The CITS Office is responsible for communicating and updating this policy as appropriate.

Attachments
None.