

**University of Massachusetts
Data and Computing Policies, Standards and Procedures Summary
University Students**

This Summary is provided to give students an overview of the University's data and computing policies and standards. All students are advised to review the [University's Data and Computing Policies/ Standards/Procedures](#) for complete acceptable use and other data and computing requirements.

The University's [Data Security Awareness and Education website](#) is another good source of information. It includes a comprehensive [Frequently Asked Questions \(FAQ\) section](#) to clarify policy, standard/guideline, and use questions.

In support of the University's mission of teaching, research, and public service, the University provides networking, computing, and a wide array of information technology to students, faculty and staff. These technology related services provide the foundation and backbone upon which all University business is conducted.

I. General

The University expects all members of the community to use computing and information technology resources in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and federal laws, and University policies and standards.

The University and/or Campus networks may enable authorized users to connect to computers at other educational and research institutions, and connect to many computers in organizations not related to the educational sector. The fact that you can connect to a computer system does NOT automatically give you authority to use that computer system. The mere lack of security on a network does not mean that a computer system is open and available for use by unauthorized users. Abuse of the networks or of computers at other sites connected to the University's computers or networks by authorized users are treated as abuse of computing resources at the University. Additionally, any network traffic exiting the University system is subject to the acceptable use policy/standards/guidelines of the network through which it flows. Note that the laws of other states may apply depending on the actual location of the computer to which the authorized user is networked (e.g., If you have connected to a computer in California, California computing laws must be adhered to. You can be prosecuted in any state through which your access flows or in which it terminates.).

All University administrative records are owned by the University Board of Trustees regardless of their physical location, even when in the possession of individuals.

The community as a whole and each individual has an obligation to abide by the following standards of acceptable and ethical use:

- Use only those information technology and computing resources for which they are authorized.
- Implement security in their daily interactions with people, data, systems, and facilities. Each person should be alert and conscious of the environment around them and notify the appropriate security/system administrators if they notice any security vulnerability.

- Use computing and information technology resources only for their intended purposes. Student access is primarily for work associated with their course of study, administrative tasks related to their association with the University (e.g., accessing their own academic/administrative data such as courses, grades) or other University sanctioned activities.
- Safeguard the integrity, accuracy, and confidentiality of University data by taking all reasonable steps to protect University data and computer systems/resources from theft; destruction; unauthorized access, creation, alteration or exposure; or any form of compromise resulting from inappropriate intentional, negligent acts, or omissions.
- Use antivirus software on any computer system they use which accesses University data or computing systems/resources.
- Contact the appropriate system, network and/or security administrators(s) prior to performing any academic game development, computer security research, or the investigation of self-replicating code as part of an academic or instructional activity.
- Follow the same standards of intellectual honesty and plagiarism in regards to software as to other forms of published work. For example, individuals should not copy another's computer file and submit it as theirs nor should they work with someone else on an assignment, sharing the computer files and then submit that file, or a modification thereof, as their own individual work.
- Notify the appropriate system, network and/or security administrator(s) of any suspected or actual security violations/incidents.
- Be aware that the University disclaims any loss or damage to software or data that results from its efforts to enforce this and other data and computing Standards.

The University makes e-mail facilities available to students. 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. Students are free to use e-mail for personal use.

File Sharing provides a convenient way to transfer information, and facilitate collaboration on projects. It can also make it convenient for a hacker or virus to invade a computer. Many of the latest viruses take advantage of shared directories that aren't adequately protected. Today's hackers can take advantage of these same vulnerabilities to place Trojans in a computer to use in gathering information and attacking other machines. The University allows file sharing, but recommends that this tool be used only when other, safer solutions, such as Secure FTP are inadequate, and that the shared folders be protected by secure passwords which are only shared with trusted friends and associates.

Possible loopholes in computer or network system security shall not be used to damage computer systems, obtain extra resources, take resources from another user, or gain access to any University computer system or any computer system networked to the University.

Created: November 29, 2007

The University recommends the installation of personal firewalls on any computer accessing University computer and network systems. Several Campuses offers inexpensive personal firewall software.

Copyrighted software shall not be copied unless explicitly allowed in the software license agreement, except for one backup copy to be made and maintained by the original licensee.

II. Individual Responsibility

Users must protect the confidentiality of personal identification codes and passwords, guard against unauthorized access to computer accounts, software, files, and other IT resources.

Authorized users are presumed to be responsible for any activity carried out under their University Logon IDs/Operator IDs/Accounts. All activity should be conducted in accordance with their role and responsibilities at the University.

Any person attaching a wireless client to any University network (wired or wireless) is responsible for the security of the device and for any intentional or unintentional activities from or to the network pathway that the device is using.

Individuals accessing University data and/or computer systems shall only access the data and/or computer systems for which they have been given authorization. This access should not be shared, transferred, or delegated.

III. Security

Never share your password with anyone or type your password when someone is watching. This includes logging on for another person and allowing them to access computer systems under your logon/operator id. Never allow anyone to access computer systems under your Account/Logon/Operator IDs. Never write down passwords or store them in batch files, automatic login scripts, terminal function keys, or in other locations where another person might discover them. Do not hard-code passwords or pin numbers used to protect access to University data in software or scripts.

Follow password security standards including, but not limited to periodically changing your computer system passwords, selecting a password that is difficult to guess and when possible, includes letters, digits and special characters (e.g., #, %, \$). Authorized user passwords must be changed periodically.

Log off computer systems/resources if you leave your pc unattended or will not be accessing data for an extended time.

IV. Privacy

University computer systems/resources may record information about each user session. Information recorded includes the username/operator id associated with the session, the login and logout dates and times, and the amount and kind of computer resources used during the session. This information is used for legitimate University purposes including issues of law, abuse, security or system managements.

The University does not routinely monitor the content of computer systems/resources including files, programs and electronic communications/emails.

The University has the authority and reserves the right to examine material (e.g., email, files, images, etc.) stored on or transmitted through its resources if there is cause to believe that the standards for acceptable and ethical use are being violated by a member of the University community, a trespasser is on its systems or networks, or for other legitimate administrative reasons. Additionally, the University has the responsibility and authority to scan computers attached to the University's wired and wireless networks to ensure appropriate security, and support network operations and performance.

The University has the responsibility and authority to release data and information to outside authorities based on bona fide requests following due legal process. The University takes steps to protect employee privacy and to ensure that protected/privileged information is not disclosed, however this privacy can not be guaranteed because the court ultimately determines whether confidential information must be disclosed.

The University takes reasonable steps to protect files stored on the university systems from unauthorized access, however, the University cannot guarantee the confidentiality of any of these files.

V. Unauthorized Activities

Individuals shall not:

- Attempt to compromise or tamper with user passwords. This includes, but is not limited to cracking, decoding, copying password files, “sniffing” packets to search for passwords or otherwise attempting to discover passwords belonging to other individuals.
- Attempt to intercept any network communication for purposes including, but not limited to: reading message/file content; rerouting packets; or packet “sniffing”.
- Remotely log into (or otherwise use) any microcomputer/PC not designated explicitly for public logons over the University and/or Campus networks, even if the configuration of the computer permits remote access, unless you has been given explicit permission from appropriate authorized personnel.
- Attempt to or obtain unauthorized access to University data, computer systems/resources, or another’s computer or email account. This includes using computing systems/resources to access any other computer system (on or off-campus) without authorization.
- Access or copy files, regardless of media (e.g., paper, diskette, etc.), of another user without prior consent from the file owner/data custodian.
- Perform or assist in the performance of any act that will interfere with the normal operation of computer, terminals, peripherals, networks, or in any activity that interferes with the rights of others such as writing/releasing viruses.
- Disseminate any Confidential information unless such dissemination is required by the individual’s job at the University.
- Post, send or publicly display or print unsolicited mail or materials that violate existing laws or University policies/standards/codes of conduct.

- “Rebroadcast” information obtained from another individual that the individual reasonably expects to be confidential.
- Illegally use, solicit or distribute copyrighted software within or outside the University, including print, audio, and video.
- Use personally owned software on University computer systems/resources unless the software is properly licensed for such use and system administrator approval has been obtained.

VI. Impersonation, Misrepresentation and Anonymity

Individuals shall not provide false or misleading information to obtain access to University computing facilities or resources nor send any electronic messages with a forged sender identity.

VII. Commercial, Political and Illegal Activities

Individuals shall not use University computer systems/resources or networks for monetary gain, political purposes or illegal activities. This includes using University Internet resources to create web pages for personal business or financial gain, except as permitted by other University policies, or to endorse or otherwise support a specific political campaign, candidate, party or referendum.

VIII. Legal Responsibilities

Individuals shall not use University data or computing resources/systems to violate state or federal laws/regulations.

Violation of University data and computing standards/guidelines may result in the loss of your computer account; disconnection from networks; your being denied or given limited access to University data, applications and/or computer systems. Individuals may be subject to reprimand, suspension, dismissal/termination, or other disciplinary action based on the offence and may be charged with criminal offenses or have civil action taken for computer abuses or violation of law within the confines of law.