

Approved: 7/13/05

University of Massachusetts Acceptable Use Summary

This Summary is provided to give students, faculty, and staff an outline of the University's data and computing policies and guidelines. All users are advised to review the University's [Data and Computing Policies/Guidelines/Standards/Procedures](#) for complete acceptable use and other data and computing requirements. Definitions related to this Summary and all Data and Computing Policies/Guidelines/Standards/Procedures are in [University Data and Computing Guidelines/Standards Definitions](#).

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 community as a whole and each individual user 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.
- 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.
- Respect the privacy and personal rights of others.

Approved: 7/13/05

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

II. Individual Responsibility

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.

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.

The University makes e-mail facilities available to both students and staff. Students may use e-mail for personal use. E-mail is made available to employees for the purpose of conducting University-related business. Occasional social/personal use is allowed providing it does not interfere with an employees' job function or performance.

III. Security

Never share your password with anyone or type your password when someone is watching. Never allow anyone to access computer systems under your 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.

IV. Privacy

The University has the authority and reserves the right to examine material 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. 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 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".

Approved: 7/13/05

- 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.
- 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.
- Illegally solicit or distribute copyrighted software within or outside the University.

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.

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.