

**University of Massachusetts  
Data and Computing Policies, Standards and Procedures Summary  
University Employees – Faculty and Staff**

This Summary is provided to give faculty and staff an overview of the University's data and computing policies and standards. All employees are advised to review the [University's Data and Computing Policies/ Standards/Procedures](#) 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.

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

Employees contacted by law enforcement to answer general questions about University systems, services, processes, etc., should refer such questions to University General Counsel.

If the law enforcement official presents a search warrant the agent or officer may begin a search as soon as the employee responding to the order has looked at the warrant and determined its scope. University employees on whom a search order is served should immediately contact their supervisor, University legal counsel and the Designated University Official at the applicable campus to inform them that a court ordered search has been requested or initiated.

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. Staff are given access to perform their job functions 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. This includes implementing appropriate physical security and data classification procedures, and periodically "refreshing" downloaded data to ensure you are working with accurate, up-to-date data.
- Properly create, access, use and dispose of University data based on the data's classification (see Attachment 1 - Data Security, Management, Use, And Disposition Requirements Based On Data Classification). Users shall access University data for approved purposes only, and shall understand the data they are accessing and the level of protection required. Databases containing Operational Use Only or Confidential data should be secured. Extracts of Operational or Confidential data should be secured at the same level as the file/database from which the data was extracted. Aggregates of data should be classified as to the most secure classification level (e.g. when data of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of classification). Reports containing Operational Use Only or Confidential data should be disposed of properly. Paper and microfiche/film should be shredded. Disks/ hard drives should be erased so as to be irretrievable.
- Appropriately backing up data (e.g., business, personal/instructional, etc.), and computer system and applications software to allow for recovery if there is a disruption.
- Using antivirus software on any computer system they use which accesses University data or computing systems/resources.
- Obtaining authorization for the processing of University data or conducting University business on home computer systems from the appropriate Data Custodian.
- Only performing remote/distributed access to administrative or research computer systems via a virtual private network (i.e., VPN).
- 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.

University departments and staff create, maintain and handle Confidential data on a daily basis to fulfill necessary University business needs. Confidential data includes personally identifiable information and protected information:

- **Personally Identifiable Information (i.e., PII)** is assigned a security classification of CONFIDENTIAL and includes University data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts. PII includes, but is not limited to:

- An individual's first name and last name or first initial and last name in combination with one or more of the following data elements: social security number, driver's license number or state-identification card number, or financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. (Massachusetts Law Chapter 93H)
- Individually identifiable health information (i.e., information relating to past, present or future physical or mental health or condition of an individual; provision of healthcare to an individual or payment for the provision of healthcare to an individual; Individually identifiable health information may include, but is not limited to: name, telephone/fax number, email address, social security number, driver's license number, internet address or any other unique identifying number, characteristic or code). Some, but not all, health information is protected under the Health Insurance Portability and Accountability Act of 1996 (i.e., HIPAA)
- Student education records not defined as student "directory information" (e.g., student number, grades, courses taken, etc.) by the University and its Campuses are protected under the Family Educational Rights and Privacy Act (i.e., FERPA).
- "Customer" records such as names, addresses, phone numbers, bank and credit card account numbers, credit histories, or social security numbers as they related to student financial aid information are protected under the Graham Leach Bliley Act of 1999 (i.e., GLB).
- **Protected Information** is assigned a security classification of CONFIDENTIAL and includes University data whose disclosure would not result in any business, financial or legal loss BUT involves issues of personal credibility, reputation, or other issues of personal privacy. The security and protection of this data is dictated by a desire to maintain staff and student privacy. Protected data includes an individual's first name or initial and last name in combination with one or more of the following data elements: their birth date, mother's maiden name, state employee salary, employee identification number, electronic signature, fingerprint, photograph or computerized image, physical characteristics or description, or passport number.

University employees have a duty to ensure that personally identifiable and protected information created, collected, used, maintained, or disseminated in the process of providing services to the public and the University community must be safeguarded against loss or theft.

The University recommends the installation of personal firewalls on all University owned systems and any computer accessing University computer and network systems. Several Campuses offers inexpensive personal firewall software to all employees for work and personal use.

Staff loaned or using University owned/funded computers (e.g., PCs, laptops, PDAs, Blackberries, etc.) shall make every reasonable effort to secure and safeguard the physical integrity of the computer and to comply with all University Data and Computing Standards.

Created: November 29, 2007

University records may not be permanently removed from the University or destroyed except in accordance with approved Record Management, Retention and Disposition Standards and schedules.

Records management is a joint responsibility of the record creator and users. All University employees who handle University records are responsible for knowing and following laws (e.g., Public Records, FERPA, etc.), University policies, guidelines/standards and campus procedures that govern these records.

Personal notes of employees are NOT subject to public record statutes, and can be maintained personally, not in "official" files.

Employees whose job functions include the transfer, donation, sale or salvage/destruction of computer hardware and/or electronic storage devices shall follow the requirements stated in the Standards for the Redistribution and Disposition of Computer Equipment and Electronic Storage Devices in addition to any campus procedures related to equipment transfer, donation, sales or recycling/destruction.

## **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.

The University makes e-mail facilities available to staff. E-mail is made available to employees for the purpose of conducting University-related business. Information resulting from communication on University computer systems is University property. Occasional social/personal use is allowed providing it does not interfere with an employees' job function or performance. Staff may use their access to University computers to use worldwide networks such as the Internet. Employees who access University or Campus networks for private purposes should subscribe to a commercial service provider.

Employees' may have personal web pages on University networks as long as they only provide information about the individual that is relevant to that individual's role at the University.

### **III. Security**

Passwords are required on all computer systems (e.g., desktops, laptops, PDAs, etc.) in which Confidential or critical data is stored or maintained.

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.

Security tokens shall not be stored with the corresponding microcomputer/pc (including transportable/laptop computers, PDAs, etc.).

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.

All University employees are under a legal duty to preserve all evidence, whether electronically stored information (i.e., ESI) or hardcopy, when notified to do so by the General Counsel's office. Failure to do so may result in fines and may jeopardize the University's position in a claim or lawsuit.

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.