

**University of Massachusetts
Data and Computing Policies, Standards and Procedures Summary
Non-IT University Departments**

General

In addition to [Data and Computing Policies, Standards and Procedures](#) impacting University employees as individuals several standards and procedures apply to Departments as a whole:

- An appropriate level of security is required on all computer systems on which Confidential or critical data is transmitted, stored or maintained.
- Departments should understand and implement University Records Management, Retention & Disposition Standards including record retention schedules in their daily business processes.
- 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 departments and 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 are safeguarded against loss or theft.

It is essential for all University departments to ensure that Confidential information, in particular personally identifiable and protected information, is secure and protected. This should start with a reevaluation of existing security controls required when personally identifiable or protected information is created, accessed, shared (electronically or in printed/fiche form) or deleted.

- University of Massachusetts departments should not use, store, or display Social Security Numbers (i.e., SSNs) unless required by law.
- University departments shall:
 - Obtain data custodian approval for the use of personal or protected data by specifying to the appropriate data custodian the purpose(s) for which personal or protected data are collected **prior** to the time of collection. Any subsequent use of the personal or protected data shall be limited to and consistent with this specification. Personal and Protected data may not be disclosed, made available or otherwise used for purposes other than that approved by the data custodian except as required by federal or state law/regulation.
 - Collect, distribute, and retain only the minimal amount of personal and protected data that is related to their business needs.
 - Collect and retain only that personal and protected data which is essential to the performance of assigned tasks.
 - Delete personal and protected information when there is no longer a business need for its retention.
 - Provide staff access to personal and protected data only as needed to perform assigned duties.
 - Design database systems so that personal and protected information can be identified.
 - When personal or protected data must be included in the distribution of data, include notification of that fact, including reference to these Standards.
 - Redact/edit out personal and protected data not critical to the task when distributing full data sets.

Created: November 29, 2007

- Be prepared to supply information needed (e.g., name, address, email) to notify impacted individuals if a data security breach occurs.
- Comply with existing University policies/standards regarding the handling of Confidential data (e.g., Do not leave Confidential data exposed on desks or computer screens left unattended; Do not send Confidential data over a public fax machine, Properly dispose of data, etc.).

Department's using computer hardware and electronic storage devices are the custodians (i.e., custodial department) of this equipment. Custodial departments are responsible for ensuring that all computer hardware and electronic storage devices under their area of responsibility are properly handled and secured from the point of delivery to the time of disposal.

Appropriate hardware and software security (e.g., cable lockdowns; password access control; data compression and encryption; audit log of access, updates; etc.) shall be placed on all microcomputers/PCs and transportable computers which have Confidential data stored in them (i.e., on the local drive).

Computer systems and networks shall have software installed and continuously enabled that will scan for computer viruses.

University computing systems may not host sites for non-University organizations across any University network unless this activity is related to the University's missions of education, research and public service including instruction, research, administrative tasks and collaborative activities with other entities, including but not limited to colleges/universities and private businesses.

Any electronic financial services (e.g., purchases of supplies, payment of student fees, etc.) provided by the University will be implemented using technically appropriate and reasonably current security technology.

All ecommerce applications must be approved and coordinated by the University Treasurer's Office to ensure compliance with Payment Card Industry standards and to ensure the use of the University approved bank for transaction processing.

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. The University and its departments license many copies of microcomputer software. The University does not own this software.

There shall be a copy of all un-networked microcomputer/PC software prior to its initial usage, to the extent consistent with applicable licenses and laws. These copies (i.e., master copies) shall be stored in a safe and secure location separate from that of the microcomputer/PC (preferably off-site). These master copies shall not be used for ordinary business, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

Critical or impacting applications (As defined in the [University of Massachusetts Business Continuity and Planning Guidelines](#)) or applications used to process administrative data that are developed on a microcomputer/PC must be developed using standard systems development life cycles and include system testing and documentation.

Created: November 29, 2007

Workstations, personal computers, transportable computers and printers housed in unsecured public areas (e.g., student labs, libraries, study rooms, etc.) shall be physically secured using appropriate security devices.

All workstations and microcomputer/PC systems are outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressers, as appropriate.

If environmental conditions pose a significant risk of static electricity discharge, all potentially effected workstations and microcomputers/PCs shall be outfitted with static protection equipment.

Proper disk maintenance practices are followed (e.g., clearly label diskettes; back up data, application and operating system diskettes; store away from extreme cold/heat; protect from dust, excessive moisture or water; keep away from magnetic devices including radios, telephones, keys, wall magnets; etc.)

Whenever a hard disk is sent for repair, the vendor shall be required to comply with [University Data and Computing Standards](#) regarding the handling of data.

Departments transferring, donating, selling or salvaging/destroying 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.

Departmental Administrator Requirements

Software upgrades address issues of incompatibility to previous versions, etc. of all supported software running on the affected computer system.

Passwords held in storage for any significant period of time or transmitted over networks should be encrypted when technically and reasonably possible.

Authorized user passwords or pin numbers must not to be sent through electronic mail unless encrypted. Information regarding a password's structure (e.g., Your password consists of your campus designation and the last 4 digits of your social security number – UMAxxxx) can be sent via electronic mail in clear text format

Departmental system administrators (e.g., email, wired or wireless networks, server, web, security, etc.) must comply with additional data and computing standards and procedures. Department heads should ensure that departmental system administrators understand and comply with applicable [Data and Computing Standards](#), [Data/System Administrator Responsibilities and System Requirements](#), [Records Management, Retention & Disposition Standards](#), etc.

Computer and network access granted to an authorized user will be prohibited in a manner which safeguards any data required to be retained, for individuals with id that remain inactive for one year; when the authorized user transfers or terminates employment, graduates or withdraws from the University; or when a "courtesy account" is inactive or no longer needed. Files of transferred or terminated employees may be reviewed and disposed of by the appropriate manager in a timely and effective manner.

Created: November 29, 2007

Application administrators shall perform risk analyses and review controls over the data system(s) under their control as part of any implementation of a new critical or impacting data system, and annually for all existing critical or impacting data system. Based on the results of these risk analyses, the administrator shall institute controls (e.g., proper backup plans, formalized restart procedures, installation of an uninterruptible power supply, etc.) which will minimize the probability that a disruption will occur and ensure quick business resumption when a disruption does occur. The costs of implementing these controls should be weighted against the loss which would result if the disruption occurred (this is referred to as risk management) and the probability of a disruption. A business resumption plan including IT recovery and business continuity should be created for all departmental applications. Specific requirements can be found in the [University Business Continuity and Planning Guidelines](#).

Web developers and designers should understand and must comply with the [Data and Computing Standards](#) related to the web.

If your department is responsible for responding to notifications of copyright or requests for network related information, appropriate personnel should understand and comply with the University [Procedures For Responding to Notification of Copyright Violation or Requests For The Content Of Electronic Communication, Any Information About Users Of the University of Massachusetts Systems/Networks, or Traffic On the University of Massachusetts Network](#).

Response to Legal Papers

University employees or departments contacted by any individual attempting to serve subpoenas or attempting to serve a civil complaint for:

- a. Student records should direct the individual attempting to serve such a notice to the appropriate Registrar or Dean of Students Office.
- b. University-related records or information other than student records should direct the individual attempting to serve such a notice to their campus Department of Public Safety/Police.
- c. Lawsuits involving the University or University departments should direct the individual attempting to serve such a notice to their campus Department of Public Safety/Police or Chancellor's Office.
- d. No employee should accept service of a subpoena or lawsuit for any other individual employee. If the lawsuit is for a Chancellor, that person's secretary can accept the notice being served.

The Department of Public Safety/Police will ensure that the subpoena is forwarded to the appropriate department head/individual (e.g., Registrar, etc.).