

Data/System Administrator Responsibilities and System Requirements

The University relies heavily on its electronic data processing systems and the data stored in them to meet its educational, research, informational and operational needs. It is essential that administrators at all levels understand their responsibilities to protect University data and the systems that process/store this data from unauthorized access or misuse and to put in place safeguards that ensure the computer systems and all data are accessed and maintained in a secure environment.

Please reference the [Data and Computing Definitions](#) for definitions of terms used throughout this document.

Table of Contents

I. PURPOSE

II. SCOPE

III. DATA AND COMPUTING ADMINISTRATOR RESPONSIBILITIES

- All System Administrators (e.g., computer, network, server, web, email, etc.)
- Wireless Network Administration
- Electronic Mail Administration
- Web Publishers, Developers and Sponsors

I. PURPOSE

These Standards are issued pursuant to the Board of Trustees' Policy Statements on [Data Security, Electronic Mail, and Computer Policy Development](#) (Doc. T97-010, adopted February 5, 1997); [World Wide Web Policy](#) (Doc. T99-059 adopted August 4, 1999); [Record Management, Retention and Disposition Policy](#) (Doc. T99-061 adopted August 4, 1999); and [Business Continuity and Planning Policy](#) (Doc. T99-060 adopted August 4, 1999). These Standards:

- Outline responsibilities related to data security; electronic mail maintenance; wireless network deployment; maintenance and monitoring; securing computer systems and their components; and documentation at the University of Massachusetts (the University);
- Define who may use the electronic mail systems controlled and administered by the University;
- Institute guidelines for the physical safeguarding of computer systems and their components; and
- Provide methods for monitoring and enforcing these Standards.

II. SCOPE

These Standards:

- Comply with and be based on the laws of the Commonwealth of Massachusetts, the United States and other regulatory agencies. This includes all applicable federal and state laws which govern the use, security, privacy and confidentiality of data, computer systems and applications, including but not limited to the Federal Copyright Law (Title 17 of the U.S. Code); Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Title 18 of the U.S. Code); Electronic Communications Privacy Act of 1986 (Public Law 99-474); the Computer Security Act of 1987 (Public Law 100-235); Family Educational Rights and Privacy Act of 1974 (as amended); the Massachusetts Fair Information Practices Act, M.G.L. c66A; Massachusetts Public Records Act, M.G.L. c. 66, section 10C; and the Computer Security Act of 1987 (Public Law 100-235). Additionally, University Guidelines/Standards and/or campus procedures may impose certain restrictions that are not specifically covered by state and federal law, or other regulations.
- Apply to all data created and maintained by the Campuses (i.e. student, research, financial, payroll/personnel, etc.) except where superseded by grant or other contracts, or by federal Copyright Law;
- Apply to all computer systems owned, leased or maintained by the University. This includes: mainframe, mini and microcomputers/PCs; servers; networks (regardless of type - LAN, WAN, etc.); routers; bridges; hubs; and various peripheral equipment including but not limited to printers and modems.
- Include all University data regardless of the medium on which it resides (e.g., paper; fiche; in electronic form on tape, cartridge, disk, CD-ROM, or hard drive; etc.) and regardless of form (e.g., text, graphics, video, voice, etc.);
- Apply to electronic mail (e-mail) and other electronic communication (e.g., “chat”, on-line conferencing, class discussions, etc.), created within, sent to, maintained within, or administered by the electronic mail systems of the University of Massachusetts;
- Institute standards for the physical safeguarding of computer systems and their components,
- Function in conjunction with other University data and computing standards/guidelines including University Information Security Policy, [Responsible/Acceptable Use of Computing and Data Resources](#) and [Data and Computing Standards](#).

III. Data and Computing Administrator Responsibilities

- **All System Administrators (e.g., computer, network, server, web, email, etc.)**

In addition to the responsibilities outlined in the [University Data and Computing Standards](#), the [Responsible/Acceptable Use of Computing and Data Resources](#), and those detailed below for specific types of administrators, all system administrators are responsible for:

- The overall implementation of/compliance to University data and computing policies, guidelines/standards and best practices for specific information systems/networks under their control (i.e., their systems);
- Understanding and complying with laws and regulations (e.g., HIPAA related to medical data systems);
- Maintaining the configuration of the system under their control as necessary;
- Developing, implementing and monitoring a computer security plan (e.g. access and environmental controls, physical and operational security, etc.) for their system(s).
- Validating an individual's identity to ensure the individual is the "owner" of a computer account prior to discussing specific user ids/accounts, user access, or resetting passwords.
- Keeping computer systems current by regularly installing "patches" or "fixes" to operating systems and applications as appropriate. When possible, released "patches/fixes" shall be reviewed and tested on a stand-alone computer system in a timely duration before being installed. "Critical security updates" shall be tested and deployed in a time sensitive manner. System patches related to any part of the system which helps process or store credit card transactions shall be made within one month of the patch becoming available.
- Addressing issues of incompatibility to hardware or previous versions, etc. of all supported software running on the affected computer system when performing hardware or software upgrades.
- Addressing hardware compatibility issues prior to purchase.
- Performing 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. Such risk analyses will determine the level of exposure to their systems, any additional controls that need to be implemented; and the appropriateness of implemented controls. University Audit or external audit firms are good resources for application administrators interested in obtaining additional or more technology specific audit/assessment checklists.
- Instituting controls, based on risk analyses performed, to safeguard data, minimize the probability that a disruption will occur, and ensure quick business resumption/recovery 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.

- Reporting the results of the risk analyses and instituted controls to the appropriate Risk Manager;
- Maintaining detailed records of risk analyses they perform and documentation of instituted controls for one year. These records/documentation should be made available to University Audit;
- Ensuring that audit trails exist for access and modification to critical operating system and network components, hardware and software;
- Taking reasonable precautions to guard against the corruption of or damage to computer systems, software, hardware or computing facilities;
- Ensuring that all hardware and software license agreements are properly executed on all systems, networks, and servers for which they are responsible;
- Clearly documenting/ inventorying, in coordination with the data custodian, all data assets (e.g., databases, data files, application and operating software, development tools and utilities, hardware, network wiring, external services, etc.) and processes on their systems;
- Documenting, in coordination with the data custodian, user access criteria (i.e., support staff access, "superuser" access, general user access, etc.) and related authorization levels for the information assets maintained in their system;
- Ensuring that all user accounts/ids on University systems have been deleted as required by University Data and Computing Standards;
- Working with the appropriate data custodian to ensure that a business resumption plan and related backup process to allow for data/email/system recovery in the event of a disruption has been developed, tested and implemented;
- Working with Investigating Teams when a data security incident takes place, and reviewing logs and observing system performance as part of their daily routine in order to route out possible vulnerabilities.
- Ensuring that problems of saturation, abuse, and malfunctioning software or hardware caused by a computer system in the system, network or security administrator's area of responsibility are addressed.
- Prohibiting all computer and network access in a manner that safeguards any data required to be retained, for individuals with logon/operator IDs on University systems when: the id has been inactive for one year; an authorized user has terminated employment, graduated or withdrawn from the University; or when a "courtesy account" is inactive or no longer needed.
- Evaluating the vulnerability of their computer systems to incoming or outgoing Internet connections or protocols, and take action as appropriate.

All devices connected to the University and/or Campus networks must conform to University data and computing guidelines/standards, campus procedures, and specific network requirements.

- **Wireless Network Administration**

The Campus Information Security Officer, in coordination with wireless network administrators, will maintain an inventory of wireless networks on their campus. Registration information will include, but is not limited to, the following information:

- Contact information for owner and responsible parties
- Location of devices
- Intended use and coverage area
- Type of wireless technology deployed
- Manufacturer name and model number
- Device description
- Service Set Identifier (i.e., SSID)/ Extended Service Set ID (i.e., ESSID), or equivalent (if applicable)
- Hopping sequence (if applicable)
- Determine what protocols and client devices are and are not supported on the wireless network.
- Provide an updated standards list that will include approved wireless technologies, acceptable RF frequencies, current minimum encryption standards, and best practices for secure installations to wireless network administrators on their campus.
- Publish a listing of equipment vendors and models that have been tested in the University environment and found to be compatible. Users may ask University network personnel to conduct certification on other equipment on a time available basis. This includes identifying wireless cards to use in desktop and laptop equipment.
- Develop a “managed guest” procedure that will include who authorizes guest access (e.g., person needs access and professor sponsors this individual for guest access), types of guest accounts (e.g., non-employee/non-student such as contractors; conferees; lecture attendees, etc.).

The Campus Information Security Officer, or their designee, may conduct periodic spectrum analysis to assess the potential impact of electromagnetic interference (i.e., EMI) from transmitters and the impact of electromagnetic emissions from WAPs.

WLAN administrators will respond to reports of wireless network service interruptions and specific devices that are suspected of causing interference and disrupting the campus/University network.

- **Electronic Mail Administration**

Electronic mail administrators are responsible for:

- Determining what categories of individuals, within the guidelines set by the President and Chancellors, may access the mail system under their control;
- Ensuring that a security plan for the e-mail system 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 **deleted and expired** mail (deleted mail includes mail in the trash folder) is not backed up for more than 30 days. After 30 days **deleted and expired** messages will be irretrievable because of resource utilization concerns. This standard applies to **deleted** mail only. It **does not** apply to mail in users mailbox or electronic mail file folders;
- 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 e-mail message retention standards, as outlined in these and other university policies/guidelines, have been developed and are implemented for their electronic mail system.

Employees responsible for maintaining, repairing and developing e-mail resources shall exercise special care and access e-mail messages only as required to perform their job function. These employees will not discuss or divulge the contents of individual e-mail messages viewed during maintenance and trouble-shooting.

Web Publishers, Developers and Sponsors

Web publishers are responsible for implementing the following standards for sites with official web pages:

- Reviewing Official University web pages to ensure that the material presented is correct and current, and complies with the official web page standards (i.e., general web standards, web design/content, and communication and application development) contained in the [University Data and Computing Standards](#) and other University/Campus publishing policies/guidelines/procedures.
- Ensuring that the web page is on-line and available to users.

Web page developers creating official University web pages will:

- Comply with the [University Data and Computing Standards](#) regarding web page development (i.e., general web standards, web design/content, and communication and application development) and any other University/Campus publishing policies/guidelines/procedures.
- Comply with the [Americans with Disabilities Act of 1990](#) (i.e., ADA) by designing web pages that are accessible (e.g., accessible to screen reading devices that are used by people with visual impairments).
- Use navigation schemes that are clear and consistent throughout campus web sites.

The web page sponsor of an official University web page will:

- Appoint a web publisher to oversee the maintenance of their page.
- Supply timely and accurate material to web page developers
- Comply with the [University Data and Computing Standards](#) regarding web page development (i.e., general web standards, web design/content, and communication and application development) and any other University/Campus publishing policies/guidelines/procedures.