

University of Massachusetts Data and Computing Standards

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. University students and staff rely on the security of the computer systems to protect instructional, research, personal, operational and other sensitive data maintained in those computer systems. It is essential that these systems be protected from misuse and that both the computer systems and the data stored in them are accessed and maintained in a secure environment.

The standards described herein are those that the University intends to use in the normal operation of its computing and network systems and facilities. This document does not waive any claim that the University may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through University computing systems.

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

Table of Contents

- I. PURPOSE
- II. SCOPE
- III. DATA SECURITY AND CLASSIFICATION REQUIREMENTS -
 - General Requirements
 - Data Classification Requirements
 - Data Security, Management, Retention, And Disposition Requirements
- IV. COMPUTER SYSTEM AND RESOURCE SECURITY REQUIREMENTS
- V. ELECTRONIC COMMUNICATIONS STANDARDS
- VI. NETWORK SECURITY STANDARDS
 - General Networks Standards
 - Wireless Networks/Technology Standards
 - Wireless Network Deployment Standards
 - Wireless Network Security Standards
 - Wireless Network Access and Use Standards
- VII. WORLD-WIDE WEB STANDARDS
 - University Web Site Structure
 - Web Pages - General Standards
 - Official Web Page - Design And Content Standards
- VIII. COMPLIANCE AND ENFORCEMENT

I. PURPOSE

These Standards function as data and computing standards and are issued pursuant to the Board of Trustees' [Policy Statement on Electronic Data Security, Electronic Mail and Computer Policy Development](#) (Doc. T97-010, adopted February 5, 1997) and [World Wide Web Policy](#) (Doc. T99-059 adopted August 4, 1999). These standards:

- Provide data security classifications for University of Massachusetts (the University) data.
- Specify how University data is to be secured, managed, retained and disposed of.
- Specify security requirements for University computing systems and resources.
- Specify capabilities required in electronic communications systems used by the University.
- Specify the requirements for using wireless technologies.
- Institute standards for the structure of the University web site(s).
- Address the development and maintenance of University web pages and applications/databases.
- Institute standards on the design and content of official University web pages.
- 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 privacy, confidentiality, security and use of data, and the use and security of computer systems and data including the Electronic Communications Privacy Act of 1986(Public Law 99-474); the Computer Security Act of 1987 (Public Law 100-235); Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Title 18 of the U.S. code); Federal Copyright Law (Title 17 of the U.S. Code); Family Educational Rights and Privacy Act of 1974 (as amended), 20 U.S.C. 1232g, and the regulations promulgated there under, 34 C.F.R., Part 99; the Massachusetts Fair Information Practices Act, M.G.L. c66A, and the Massachusetts Public Records Act, M.G.L. c. 66, section 10. If this Guideline conflicts with federal or state statute, the applicable statute shall apply. Additionally, other University Policies, Guidelines/Standards and/or campus procedures may impose certain restrictions that are not specifically covered by state and federal statute or regulations (e.g., [University Trademark and Licensing Policy](#), [Business Continuity and Planning Guidelines](#), etc.).
- Apply to all University staff, students, authorized users, contractors and visitors that have access to University facilities, computing resources or University data.
- 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;

- 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 all computer systems owned, leased or maintained by the University. This includes: mainframe, mini and microcomputers/PCs; servers; networks (e.g., LAN, WAN, WLAN, wired, wireless, etc.); wireless access points (i.e., WAPs), wireless phones (excluding cell phones), routers; bridges; hubs; and various peripheral equipment including but not limited to printers and modems.
- Apply to all wireless network access devices and technologies that provide a bridge between the University's wireless and wired networks (hereafter "wireless access points"), or any device that is designed to communicate with such a device via the University's wireless network (i.e., wireless client).
- Apply to all University wireless local area network (i.e., WLAN) technologies, both inside buildings (including residence halls) and in outside areas.
- Apply to all Web pages and applications contained on University equipment or disseminated via University resources.
- Refer to all data as defined in the [Data and Computing Definitions](#).
- Function in conjunction with other University data and computing guidelines/standards including the [Responsible/Acceptable Use of Computing and Data Resources](#) and [Data/System Administrator Responsibilities and System Requirements](#).

III. DATA SECURITY AND CLASSIFICATION REQUIREMENTS

General Requirements

University data, regardless of its medium and/or form, shall be:

- Identified as to its classification (i.e. Unclassified, Operational Use Only, or Confidential);
- Protected in a manner which is commensurate with its classification and value;
- Appropriately secured and not accessible to non-approved users when not in use;
- Safeguarded by security systems designed for the protection of, detection of, and recovery from the misuse of information resources. Such security systems will ensure the quality, integrity, and availability of University data
- Made secure against unauthorized creation, updating, processing, outputting, and distribution;
- Accessed, used and disposed of in a manner commensurate with the data's classification and with [University Records Management, Disposition and Retention Standards](#), [University and Departmental Records Retention & Disposition Schedules](#) and Campus procedures;
- Disseminated by officially designated offices only,

All computer access granted to an authorized user will be removed when that user terminates employment, graduates, or withdraws from the University, or when their courtesy account is inactive/unneeded.

Data Classification Requirements

University data classifications must be adhered to. Three levels of data classification have been established. The data classifications DO NOT apply to correspondence or memorandum **EXCEPT** when the correspondence/memorandum contains other than unclassified data.

The data classifications determine how the data will be secured, managed, retained, and disposed of. Dissemination of University data to external sources is dictated by the Family Educational Rights and Privacy Act of 1974 (as amended), 20 U.S.C. 1232g, and the regulations promulgated there under, 34 C.F.R., Part 99; the Massachusetts Fair Information Practices Act, M.G.L. c66A, and the Massachusetts Public Records Act, M.G.L. c. 66, section 10. Assignment of data into the following classifications shall be performed in accordance with the requirements of the foregoing laws.

- **Unclassified** - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific data custodian approval.
- **Operational Use Only** - data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss BUT which the University had determined is critical to its business and requires a higher degree of handling than unclassified data. Access to Operational Use Only data is available to data custodian approved users only.
- **Confidential** - data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts (i.e., protected data); personally identifiable data; data that involves issues of personal privacy; or data whose loss, corruption or unauthorized disclosure may impair the academic, research or business functions of the University, or result in any business, financial, or legal loss.

See [Attachment 1](#) for table of Data Security, Management, Use, And Disposition Requirements Based On Data Classification.

Data Security, Management, Retention, And Disposition Requirements

University data will be secured, managed, handled and disposed of based on the data classification.

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.
- 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.).

Data custodians should understand that signature imaging is not a secure method of authorization. Custodians should seek the level of secure authorization most appropriate for their data's classification

Access to data classified as Operational Use Only and Confidential shall be approved by the appropriate data custodian based on legal requirements or a need to know, job function or course requirement basis.

Programs and files are Confidential unless they have explicitly been made available to other authorized users.

An appropriate level of security is required on all computer systems on which Confidential or critical data is transmitted, stored or maintained.

To the extent technically and reasonably possible, all Confidential data:

- Shall contain audit trails to monitor access and modification, and is appropriately backed up to allow for recovery;
- Stored on workstations or microcomputers/PCs and not backed up centrally on a network, shall be backed-up on separate storage media after changes to the data have occurred. Backups should be stored in an off-site location. Additionally, backups of Confidential data shall not be used for data restoration purposes unless another back-up copy of the same data exists. This will prevent the only current copy of Confidential data from being inadvertently damaged in the restoration process.
- Transmitted over any communication network shall be transmitted in encrypted form or other appropriate and equally secure method.
- Will only be accessible on the WWW with the permission of the appropriate University data custodian. WWW access to such data shall be secured in a manner that is commensurate with the classification and confidentiality of the data contained on the page/publication.

Passwords are required on all computer systems (e.g., desktops, laptops, PDAs, etc.) in which Confidential or critical data is stored or maintained. Exceptions to the password requirement are access to worldwide web products.

Passwords and Pin numbers used to access Confidential data and computer system passwords on administrative or research computers should be a minimum of 6 characters.

Wireless networks should employ a combination of layered authentication methods to protect Confidential data.

Any Web server storing Confidential Data, even on a temporary basis, must adhere to these and other University data and computing guidelines/standards and ensure that the data is secured in a manner commensurate with the data's classification

All Applications/databases (including web based) which access Confidential data shall support and include:

- User authentication
- A level of security that ensures only authorized users have approved access (i.e., view, update) to appropriate data.
- Inter-system communication security among different servers or systems that store or access the data.

- Journaling and transaction logging at a level that would record both successful and failed authentication attempts, the related IP addresses, date and time.
- Monitoring
- Trace facilities

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).

Vendors, contractors, consultants and external auditors needing access to University data must read and acknowledge in writing that their firm has read, understood and will comply with all University data and computing guidelines/standards.

IV. COMPUTER SYSTEM AND RESOURCE SECURITY REQUIREMENTS

The following computer system and resource security requirements or a documented, equivalent compensating control shall be implemented:

Administrative and research computer systems, and networks carrying administrative or research data must contain secured audit trails to monitor access and modification to critical operating and network system components.

Computer system and application software will be appropriately backed up to allow for recovery if there is a disruption. Multiple generations of operating system, application and data backups should be maintained in both on-site and off-site storage facilities.

All vendor-supplied default passwords are changed before any computer or communications system, printer, copier, fax machine or other equipment is used for University related business.

Authorized user logon ids/operator ids on administrative and research computer systems are inactivated or an authorized user's access connection is immediately terminated if the authorized user does not provide a correct password after five (5) consecutive attempts.

Passwords or pin numbers used to protect access to University data are not hard-coded into software/source code developed by University staff or students.

The display and printing of passwords or pin numbers shall be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

When technically and reasonably possible,

- All administrative and research computer systems must display a notice at log-in (i.e., login banner) stating that the system is to be used by authorized users only and that by continuing to use the computer system, the individual represents themselves as an authorized user;
- All administrative and research computer systems must give information reflecting the last log-in time and date to every user at the time of log-in;
- Computer system "idle time" or "time-out" capabilities shall be implemented on administrative and research computer systems, and on networks carrying administrative and research data;
- Computerized password creation checking is implemented for administrative and research computer systems.
- Single-sign on processes. Authorized user identity and access related information should be user-transparently passed to other computers, networks, database management systems, and applications.

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.

All uses of encryption should employ standard encryption algorithms (such as the DES, PGP, or EDE), standard implementations (such as cipher-block chaining), and standard security practices (e.g., periodic changes, appropriate lengths, etc.). This will ensure interoperability, lower costs, and facilitate secure business processes.

Access to encryption keys is strictly limited to those who need to know this information in order to perform their job function. Consultants, contractors, or other third parties should not be given access to encryption keys unless approved by the appropriate Chancellor or their designee.

University encryption systems must be designed such that no single person has full knowledge of any single encryption key. Additionally, automated encryption management processes should be employed where reasonably possible and encryption keys should only be transmitted over communication lines or stored on computer storage media in encrypted form.

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

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

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

Authorized users are assigned unique logon IDs or operator IDs, and passwords/pin numbers to access University computers, networks and their application systems and data. Users accessing non-University systems (e.g., World Wide Web) may be given network logon IDs.

Authorized user passwords are changed periodically.

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.

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.

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.

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. This ensures that the discharge of static electricity does not damage computer equipment or data.

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.

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.

When disposing (e.g., recycling, salvaging, transferring ownership to another party, etc.) of microcomputer/PC hard disks, the hard disks should be wiped to make the data irretrievable.

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

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.)

V. ELECTRONIC COMMUNICATIONS STANDARDS

Communication systems, regardless of the tool used (e.g. electronic mail packages, Web features, client-server products, etc.), that are employed by the University to communicate with staff, students, other campuses, etc. will support the following capabilities whenever technically and reasonably possible:

a. Communication Systems – Required Features

- Word-Processing-like edit capabilities
- Ability to attach documents via a graphical user interface (GUI). For example, Word, Excel, binary attachments such as gifs, executable programs, videos, etc.
- Public/group level posting capability (i.e. Bulletin Boards/Newsgroups)
- Campus and Central Administrative Services directory information will be available to authorized users.
- Directory information available to authorized users will include mail address, name, campus, department name, and campus postal address. Each campus must be capable of excluding from any such directory entries for those students who exercise their rights under the Federal Educational Rights and Privacy Act, 20 U.S.C. § 1232g, to request that their directory information be withheld from release.

- Multipurpose Internet Mail Extensions (MIME compliant)
- Public and private mailing lists
- Electronic file folders
- Context-sensitive help
- Remote access (dial-in, network, etc.) to e-mail
- Ability to send electronic mail over the Internet
- User customizability of options/features (personalize the client)
- New mail notification
- Application program interface (API)
- Signature block
- Web enabled features
- Customizable feature control (user profiles, etc.)
- Ability to facilitate access by disabled authorized users using reasonably current technology.
- Platform independent client access
- Compatible with current open industry standards

b. Communication Systems - **Preferred Features**

- . Electronic forms support
- . Scheduling capability (calendar)
- . FAX capability
- . Conference chat
- . Authenticated Digital Signatures
- . Access through Secure Sockets Layer (SSL)

VI. NETWORK SECURITY STANDARDS

General Networks Standards

Wired and wireless networks are viewed the same and, therefore, must comply with any and all University guidelines/standards related to University networks and computer systems.

The University has the responsibility and authority to scan computers attached to the University's networks to ensure appropriate security, and support network operations and performance. The University reserves the right to restrict access to services and resources that are disruptive to its networks, or pose a threat to the University's information security, audit or accreditation status.

Network connections are deployed to benefit the entire University and support its 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. These network connections are not to be used to provide commercial services not related to the University's missions as noted above nor shall they be used in any illegal activities.

Network wiring, component, software and hardware requirements shall be documented for all University networks.

University and Campus networks should be designed and implemented to the extent technically and reasonably possible so that:

1. No single point of failure, such as a central switching center, could cause network services to be unavailable.
2. Critical communications may immediately be sent via multiple long distance carriers over physically diverse routes.

Application and systems software available over a University network must be handled in a manner that does not result in the number of copies/simultaneous users dictated in the software license being exceeded.

All non-software proprietary information (e.g., text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with laws.

All inbound dial-up lines (e.g. modems) and real-time external connections (e.g., Internet) connected to University networks carrying administrative or research data must pass through an additional access control point (e.g., firewall) before authorized users reach the log-in banner.

All in-bound dial-up lines to administrative and research computer systems shall be protected with extended user authentication systems as technically and reasonably possible.

Access security controls must uniquely identify each remote access user, device and port.

Both ends of a dial-up connection shall be dropped when the access session is terminated.

Direct network connections (e.g., a tunnel) between any University network carrying administrative or research data and computers at external organizations via the Internet or any other public network, are prohibited unless specifically approved by the appropriate Chancellor, or their designee.

All user-initiated commands received from locations other than University administrative networks shall not be fulfilled unless a user has first logged in. This will result in commands such as the "finger command" not being able to be used to obtain information which can then be used to obtain logon/operator ids and passwords.

Adequate controls exist to restrict access to and use of network troubleshooting equipment (e.g., protocol analyzer), audit (e.g. COPS, ISS, Tripwire, etc.) and network management software (e.g., SATAN, etc.)

All University buildings will be wired in a manner to support a modern, high speed, computer

Wireless Networks/Technology Standards

Wireless network devices offer a simple, convenient, and inexpensive solution to extend network accessibility by reducing the requirements of physical infrastructure. Wireless networking removes the encumbrance of wire connections on portable devices, and can also enable laptop and handheld users the ability to travel beyond traditional network boundaries (e.g. between buildings, in outdoor spaces, etc.) without losing network connectivity. Please note however, wireless networks do not replace wired networks. Wireless networks do not offer the same performance, stability or security as wired networks. Wireless networks are a convenience tool only.

Wireless technologies afford a great opportunity for the University community. However, such technologies must be deployed to ensure that an acceptable level of integrity, reliability, service quality and security exist. A structured wireless deployment will ensure that:

- Interference between different departmental implementations and other uses of wireless spectrum is mitigated.
- The security of University data, networks and computer systems is safeguarded.
- A baseline level of connection service quality is provided.
- The wireless network interacts optimally with the wired network.

The wireless network should be thought of as an extension of the wired network to promote mobility. The requirements set forth in these as well as other University guidelines/standards, apply to the wired and wireless networks, however, there are special concerns in the wireless environment that need to be addressed. This section outlines the processes, requirements and standards needed to implement a secure, reliable and usable wireless network at the University.

Wireless Network Deployment Standards

All WAPs must be registered with the campus information security officer at the time of deployment in the UMass environment.

All Supervisory Control and Data Acquisition (i.e., SCADA) devices must be registered with the campus information security officer at the time of deployment in the University of Massachusetts environment.

Only approved and registered WAPs will be deployed within the UMass system.

In order to minimize interplay and possible interference with existing wired and wireless networking infrastructure only authorized staff will install wireless networking ‘access points’.

Final device names will be assigned during the registration process to avoid conflicts and confusion, and to aid the campus information security officers in identifying and locating WAPs.

Wireless applications will be deployed in a manner to prevent interference between the University wireless network infrastructure and other uses of the wireless radio spectrum.

In cases where WAPs have variable radio power levels, the minimal power level that provides the intended coverage should be chosen so as to limit interference with other devices operating in that frequency range.

All radio-based products being installed must comply with both the [ANSI C95.1-1991 IEEE Standards for Safety Levels with Respect to Human Exposure](#) as well as the [FCC Office of Engineering and Technology Bulletin 65 Evaluating Compliance with the FCC Guidelines for Human Exposure](#). The radios must be evaluated by the vendor for RF Safety Compliance per the requirements of FCC Part 2.1091 and 2.1093 of the FCC Rules. Wireless access points must be designed to reduce emissions that can interfere with medical devices. Access points in public areas must meet the FCC requirements for devices operating in medical environment specifically EN 55011 emission standards.

Any new construction plans should be evaluated for consideration of new or updated wireless networking

Wireless Network Security Standards

Wireless access points should be installed in physically secure areas accessible only by authorized personnel to prevent unauthorized access and physical tampering. Devices should not be placed in easily accessible public locations. If the device must be installed in an open area, it will be located at a height of 12' or greater, where technically possible.

Wireless clients accessing the campus wired infrastructure must meet certain data networking and security standards including but not limited to IEEE 802.1x (Port Based Network Access Control) to ensure that authorized and authenticated users are able to connect to the campus network and that University computing resources are not exposed to unauthorized users.

Due to the inherent security risks with wireless, it is strongly recommended that additional security layers be implemented on top of the 802.1x security model. The University should deploy "modern and current" technologies for wireless encryption. Examples of this include EAP standards which use strong mutual authentication, support open authentication, use key management, use key rotation, and use WPA1 or WPA2. Both WPA1 and WPA2 provide significantly stronger encryption than does the WEP standard. The most current version (WPA2) supports CCNP, which is based on AES encryption and is (as of this writing) the current gold standard in the wireless encryption realm. This list is not intended to be comprehensive nor exclusive of new security technology that is developed.

In cases where the client's EAP standard only supports the common username and password model, passwords must be long, nonmeaningful strings of characters, including letters, numbers and symbols.

Only WAPs that support power level adjustment may be used, and that feature must be used to minimize the overlap of legitimate networks and prevent radio signals from spilling into unintended areas.

All WAPs must be secured using an administrative password.

Wireless network administrators shall ensure that all vendor default usernames have been removed from deployed wireless devices, when technically possible. All default passwords, SNMP community strings, and other remote-management authentication mechanisms must be changed from their defaults prior to deployment onto the production network. Default SSIDs set by the manufacturer will be changed prior to device deployment.

In order to make it difficult for unauthorized users to learn the network name and attempt an attack or intrusion campus information security officers should ensure that security features available with WAPs are enabled. Many embedded security features are disabled by default and need to be “turned on” prior to deployment.

Administration of wireless devices should be prohibited from the wireless network.

Wireless networks must traverse a routed network interface before logically contacting a traditional wired network.

Access control and security mechanisms such as gateways, firewalls and network-based intrusion-detection systems should be deployed. This will separate the wireless network from the internal wired network and detect system compromise if they occur. System logs should be monitored weekly and critical host logs should be scanned daily.

Device installers must ensure the wireless device is properly secured prior to deployment. Once deployed, the responsible campus information security officer, or their designee, shall perform a security analysis using current wireless security methods. The responsible campus information security officer, or their designee, shall also perform periodic security verifications.

Wireless clients should include proper security controls such as virus protection, password and other preventative measures. When possible, security patches, upgrades, and antivirus software updates should be pushed to clients from servers.

Wireless Network Access and Use Standards

All access via the wireless infrastructure requires user authentication.

Once authenticated to an access point, authorized users must either be routed outside the UMass firewall(s), or authenticate to a University network.

Wireless clients must not be used for connecting to campus business systems such as PeopleSoft Human Resources and Financials, student information, patient records including MediTech and IDX, or other systems that contain Confidential data, or are critical to the mission of the University unless using encryption protocols or other appropriate and equally secure methods,

and secure transport protocols such as SSL (Secure Sockets Layer) or IPsec. No portion of access to these systems, or saving / printing related data will be conducted on a wireless medium without appropriate security. Additionally, wireless access points will be programmed to disallow access to high risk services noted above (e.g., PeopleSoft Human Resources and Financials, student information, patient records, etc.) unless the user is using encrypted protocols.

Wireless transmissions must not be used in prohibited areas, or where interference with other electronic equipment could be a problem.

Applications access via the wireless infrastructure shall include appropriate password and data protection controls.

Research groups and labs should be aware that conditions of some federal grants include data confidentiality and protection. No data or network protection can be guaranteed on wireless networks.

VII. World-Wide Web Standards

The Standards set forth in this section supersede conflicting guidelines/standards or procedures developed for individual web sites/servers.

University Web Site Structure

Each Campus and the President's Office shall publish an official University web page.

All official web pages shall be hosted on a University of Massachusetts domain name space unless prior approval is obtained from the campus Chief Information Officer.

One web page will be recognized as the homepage of the University.

All official web pages will be linked to the appropriate campus' homepage (e.g., Amherst Campus related pages/publications should contain a link to the Amherst Campus homepage).

Campus procedures will ensure that the Campus homepage will provide a clear outline of that Campus' web organization and easy links to a campus organization chart.

Each campus homepage will be linked to a search engine that has access to the official University web pages of that campus. The President's Office homepage will be linked to a search engine that has access to the official University web pages on the President's Office web site, and the University homepage will be linked to a search engine that has access to the official University web pages on the University web site.

University web pages (i.e., Official or Unofficial web pages) and applications/databases may be located on any University web site/server.

Web applications, scripts, related databases, libraries, and other files must be secured in a manner that prevents unauthorized access to the server file system, configuration, or operating system.

Web Pages - General Standards

All official campus documentation must be published via the Web and only becomes “official” once it is published and adheres to the standards outlined in this document and any other related Guideline or Campus Procedure. Given the near zero-cost and immediacy of Web publishing, publishing official university materials via official University web pages is the most practical means of communicating change. Other methods might rely on longer publishing schedules and thus new information is not readily communicated to students, faculty and staff.

All University Web Pages are either Official University Web Pages or Unofficial University Web:

a. **Official web pages** are those web pages on University web servers that have been created by/for the University, its campuses, colleges, schools, departments or other administrative offices, for University business. Official web pages **DO NOT** include, among others, web pages and applications created by individual faculty, staff, students or student organizations. Official web pages shall contain the statement, “**This is an Official Page/Publication of the University of Massachusetts** _____ (Campus, unit name - e.g., Amherst Campus English Department) and must meet University guidelines/standards for design and content.” The word “Official” in the statement above will link to a page containing the following disclaimer:

As a service and for informational purposes only, the University may provide listings of and/or links to web pages maintained by University faculty, staff, students, student organizations, non-university organizations and others. The University is not responsible for and does not monitor the content or administration of these pages. These pages and their content, including but not limited to factual statements and opinions, are the sole responsibility of their creators and do not represent, explicitly or implicitly, positions, policies or opinions of the University of Massachusetts.

Additionally, the campus designation in the statement above (e.g., Amherst Campus) will link to the appropriate Campus’ primary homepage.

b. **Unofficial web pages.** All web pages that are not official web pages are Unofficial web pages and are not reviewed or monitored by the University.

The University reserves the right to remove from University web sites/servers or otherwise prevent the dissemination through University resources any web page that violates or contains material in violation of University Policy, Guidelines/Standards, Campus procedures or the laws and regulations of the United States, the Commonwealth of Massachusetts, or any other political division of competent jurisdiction. Additionally, University data and computing

guidelines/standards may impose certain restrictions that are not specifically covered by state and federal law, or other regulations. The University does not represent by this or any other statement that it shall monitor or assume responsibility for the content of any Unofficial web page.

Limitations on the size and number of unofficial web pages may be imposed if resources become overburdened.

Official Web Page - Design And Content Standards

Because the quality and accuracy of information published by the University (and on University Web servers) directly affects its reputation and image it is essential that such information follow minimal guidelines/standards of content and structure. It is also essential that information published electronically is consistent with the same high standards as other forms of published information (e.g., print, audiovisual, etc.). The official web page design and content standards have been developed to provide an overall standard design for official pages/publications while also providing for the individualization of campuses, departments, and other University related organizations (e.g., official committees or task forces, major service units, etc.). These standards in no way intend to limit these areas ability to produce their own material.

Official web pages shall:

- a. Be created for the purpose of carrying out official University business.
- b. Be approved by the Campus or Central Administrative Services information security officer, as appropriate.
- c. Contain the statement, **“This is an Official Page/Publication of the University of Massachusetts _____”** (Campus, unit name - e.g., English Department). Additionally, the word “Official” is the statement above will link to a page containing the following disclaimer:

As a service and for informational purposes only, the University may provide listings of and/or links to web pages maintained by University faculty, staff, students, student organizations, non-university organizations and others. The University is not responsible for and does not monitor the content or administration of these pages. These pages and their content, including but not limited to factual statements and opinions, are the sole responsibility of their creators and do not represent, explicitly or implicitly, positions, policies or opinions of the University of Massachusetts.

Additionally, the campus designation in the statement above (e.g., Campus, unit name) will link to the appropriate Campus’ primary homepage.

- d. 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). Web page developers should be aware of the [World Wide Web Consortium Web Content Accessibility Guidelines](http://www.w3.org/TR/WCAG10) (<http://www.w3.org/TR/WCAG10>) when developing accessible web pages.

e. Contain the following basic components:

- The title of the web page, subtitle (if any) and the name of the organization/department/unit publishing the page. This title should appropriately describe the content of the page.
- A link to a form or an email address identifying the web page contact so that questions, corrections, or comments can be appropriately directed.
- The last revision date.
- Links to the campus or University homepages, as appropriate.

f. Point to resources available at other campuses and within Central Administrative Services as appropriate.

g. Use text-labeled button bars or other navigation aides. Pages should not contain items that look like buttons but do not work like a button.

h. Be designed to address the issues of varying user screen resolution and the slow loading of images.

i. All navigational aids which are inline images or image maps should also contain alt tags giving equivalent informational or navigational functions for users of web browsers that can't display images. The provision of a text description for any information-bearing graphic is critical for accessibility. These text descriptions are most commonly supplied by using "alt tags" in HTML. The text can be displayed by non-graphical.

j. **Not** have dead-end or malfunctioning links.

k. Comply with any other pertinent University policies/standards/guidelines (e.g., [University Trademark and Licensing Policy](#), etc.) or Campus procedures.

l. Contain no statements of a fraudulent, defamatory, harassing, abusive, obscene or threatening nature. Such information will be removed from display. Additionally, the University has special concern for incidents in which individuals are subject to harassment or threat because of membership in a particular racial, religious, gender or sexual orientation group.

m. Comply with HTML standards as defined by the [World Wide Web Consortium](http://www.w3c.org) (<http://www.w3c.org>).

- n. Be cross-browser compatible with the most popular browsers especially in regard to client-side scripting languages.

Official web pages may contain external advertising if University policy allows such advertising in print media and only if such advertising is specified pursuant to a valid contractual agreement between the University and a third-party.

VIII. COMPLIANCE AND ENFORCEMENT

In addition to the standard compliance and enforcement statement detailed in the University [Responsible/Acceptable Use of Computing and Data Resources](#) and [Data/System Administrator Responsibilities and System Requirements](#) documents, the following compliance and enforcement processes are available:

Where interference between the campus/University network and other devices cannot be resolved, the University reserves the right to restrict the use of all wireless devices in University owned or leased buildings, and all outdoor spaces.

In cases where the interfering device is being used for a specific academic application, the network administrator will work with the user to mitigate the interference and accommodate the device without disrupting the University WLAN(s). In the event that both cannot operate without interference, use for specific teaching or research applications will take precedence over the general access WLAN. The campus CIO has the authority to require cessation of unauthorized use of wireless devices.

WAPs determined to be interfering with the wired network or other wireless devices may be disconnected and removed so as to eliminate interference with other devices and services. This includes registered and non-registered (i.e., rogue) access points.

Web pages that do not comply with these Standards may be modified, removed or otherwise rendered inaccessible from University web site/server. This may involve removing links, direct editing or requesting the appropriate system administrator to halt access to the server hosting the web page.