Doc. T97-010
Passed by the BoT
2/5/97

UNIVERSITY OF MASSACHUSETTS
POLICY STATEMENT ON DATA SECURITY, ELECTRONIC MAIL, AND COMPUTER POLICY DEVELOPMENT

The President of the University shall ensure that each campus institutes data security, electronic mail and computer policies, and, from time to time, amends them as appropriate or as required by law. If any campus policy conflicts with federal or state statute, the applicable statute shall apply.

The President, together with the Chancellors or their designees, shall establish standards and timetables for electronic data security, electronic mail and computer policy development on the campuses. Campus policies must adhere to these standards.

UNIVERSITY OF MASSACHUSETTS
COMPUTER SECURITY AND USAGE GUIDELINES
(Doc. T97-010)

GUIDELINES

University computers and computer related resources are valuable assets that are relied upon heavily for academic, information and decision-making 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 be accessed and maintained in a secure environment.

I. PURPOSE

These Guidelines 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:

- ensure the ethical, legal and responsible use of University of Massachusetts (the University) computing resources;
- outline responsibilities related to the accessing and usage of computers at the University;
- institute guidelines for the physical safeguarding of computers and their components; and
- provide methods for monitoring and enforcing these Guidelines.

II. SCOPE

Campus procedures regarding computer security and usage shall:

- comply with and be based on the laws of the Commonwealth of Massachusetts and the United States and other regulatory agencies. This includes all applicable federal and state laws which govern the use and security of computer systems and data, including 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); Electronics Communications Privacy Act of 1986 (Public Law 99-474); and the Computer Security Act of 1987 (Public Law 100-235). Additionally, University Guidelines (Data Security & Classification Guidelines, Electronic Mail Guidelines, etc.) and/or campus procedures may impose certain restrictions which are not specifically covered by state and federal law, or other regulations;
- apply to all computer systems owned, leased or maintained by the University. This includes: mainframe, mini and microcomputers; servers; networks; and various peripheral equipment including but not limited to printers and modems;
- apply to all authorized users of the University's computer systems.

III. RESPONSIBILITIES

The President, together with the Chancellors, will ensure that:

- appropriate and auditable internal controls; and
- appropriate and tested business continuity plans;
- are in place for the computer systems at the University.

Campus procedures regarding computer usage will establish mechanisms to determine which University department(s) shall be responsible for specific computer systems.

The individual assigned responsibility for specific computer system(s) will assign technical and security responsibilities to a system and/or security administrator. This may be the same person and may be part of the University's or Campuses' computing departments and not part of the specific department responsible for the computer system.

Campus procedures regarding computer security and usage shall require that system and security administrators are responsible
for:

- developing, implementing and monitoring a computer security plan (e.g. risk analysis, access and environmental controls, physical and operational security, etc.) within the extent of these Guidelines for the system(s) under their control;
- developing, implementing and testing a backup plan in order to allow for the recovery of University computer systems in the event of a disaster;
- ensuring that audit trails exist for access and modification to critical operating system components;
- taking reasonable precautions to guard against the corruption of software, or damage to hardware or computing facilities;
- periodically evaluating the level of risk within the computer system (e.g., network, server, mainframe, etc.) and taking action, as needed;
- ensuring that all hardware and software license agreements are properly executed on all systems, networks, and servers for which they are responsible;
- ensuring that authorized user passwords are changed periodically;
- implementing computerized password creation checking on administrative and research computer systems, when technically possible;
- implementing "idle time" or "time-out" capabilities on administrative and research computer systems, when technically possible;

- deleting all computer access for individuals with logon/operator IDs on University systems when: an authorized user has terminated employment, graduated or withdrawn from the University, or when a "courtesy account" is inactive or no longer needed;

- developing, distributing and enforcing procedures, consistent with procedures provided by the appropriate campus Chancellor, for the reporting and follow-up of security violations;

- developing, presenting and maintaining security awareness programs and training for authorized users. This includes developing methods to ensure that information regarding computer security, and applicable laws, regulations, policies, and procedures are distributed and available to authorized users.

Campus procedures regarding computer security and usage shall require that authorized users:

- follow password security standards including, but not limited to:

    1. periodically changing their computer system passwords;

    2. selecting a password that is difficult to guess. Logon/Operator Ids, names, birth date, social security number, repeating characters (e.g., 111111 or ababab), common character sequences (e.g. "123456" or "abcdef"), or common words that can be found in a dictionary are prohibited;

    3. sharing or giving anyone else permission to use their logon/operator IDs or passwords is prohibited;

    4. storing access passwords in batch files, in automatic login scripts, in terminal function keys, in computers without access control or in other locations where another person might discover them is prohibited;

    5. sending access passwords through electronic mail is prohibited.

- exercise responsible, ethical behavior when using University computing resources;

- safeguard computer resources from theft; destruction; unauthorized alteration or exposure; or any form of compromise resulting from intentional or unintentional sources;

- notify the appropriate security/systems administrator of any apparent or actual security violation.

Campus procedures regarding computer security and usage shall require that authorized users will **NOT**:

- intentionally damage or misuse any University computer system including terminals, microcomputers, printers or other associated equipment;

- intentionally write, produce, generate, copy, propagate or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software unless such action is part of authorized research or testing. Such software is often referred to as a virus, worm, Trojan Horse, or some similar name;

- use University computer systems and their applications in illegal activities;

- attempt to intercept any network communication for purposes including, but not limited to: reading message/file content; searching for passwords; rerouting packets; or packet "sniffing";

- access or copy files, regardless of media (e.g., paper, diskette, etc.), of another user without prior consent from the file owner. Accessing the "private" files of others without permission, even if those files are unprotected, is prohibited. Altering another user's files or systems files without permission is vandalism and destruction of University property;

- attempt to develop or use any mechanism to alter or avoid charges levied by the University for computing resources;

- use personally owned software in University microcomputers unless the software is properly licensed for such use;

- copy or remove software from University microcomputers in violation of the software license. This includes copying software from or to University microcomputers;

- illegally distribute copyrighted software within or outside the University through any mechanism, electronic or otherwise;

- unnecessarily or inappropriately use limited computer resources;

- use public, lab or departmental equipment for personal entertainment when other authorized users need access to perform University related tasks;

- print excessive copies of documents, files, data or programs.

Campus procedures regarding computer security and usage shall require that all University students and employees:

- are appropriately oriented and sign a computing awareness and data security compliance statement which includes the language in Attachment 1 of these Guidelines; and

- reaffirm annually that they know and understand University policies/guidelines and campus procedures regarding data and computer use.

IV. COMPUTER SYSTEMS AND SOFTWARE

Campus procedures regarding computer security and usage shall require that:

- Only systems/security administrators or their designees can modify the configuration of the University or Campus computing infrastructure by adding or removing network links, computers, or peripherals;

- Appropriate physical security standards are in place;

- Administrative and research computer systems contain audit trails to monitor access and modification to critical operating system components;

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

- Passwords are required on all computer systems in which confidential or critical data is stored or maintained. Exceptions to the password requirement are access to gopher or world-wide web products;

- Pin numbers used to access Private, Restricted or Confidential data, and computer system passwords on administrative or research computers should be a minimum of 6 characters;

- Computerized password creation checking is implemented for administrative and research computer systems, when technically possible;

- Computer system "idle time" or "time-out" capabilities are implemented for administrative and research computer systems, when technically possible;

- Computer systems and networks have software installed that will scan for computer viruses;

- Copyrighted software is not 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. Employees and students are required to comply with software licenses and the U.S. Copyright Act;

- Shareware and public domain software are properly used. The University encourages the use of shareware and public domain software however, the use of such software should be predicated on the fact that it has been scanned for computer viruses;

- System/security administrators evaluate the vulnerability to their computer systems by incoming or outgoing Internet connections or protocols, and take action as needed.

V. ACCESS

Access may be given to: stand-alone micro, mini or mainframe computers; or to networked computer systems. Student access is primarily for work associated with their course of study, activities related to courses, or administrative tasks related to their association with the University (e.g., accessing their own academic/administrative data such as courses, grades). Staff are given access to perform their job functions. Students and staff may however, use their access to University computers to use world-wide networks such as the Internet.

Campus procedures regarding computer security and usage shall require that:

- Authorized users understand that by using any University computing system, the user agrees to comply with this and all University computing related policies/guidelines such as the Data Security and Classification Guidelines and the Electronic Mail Guidelines. Also, as a condition of obtaining access to any University computer system, all authorized users are required to sign a computing awareness and data security compliance statement (Attachment 1) that they have received a copy of and read these Guidelines, understood them, and will comply with them;

- Only authorized users have access to University computer systems;

- Individuals requesting access to University computer systems, will not provide false or misleading information to obtain access to University computing facilities;

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

- Individuals will not attempt to compromise authorized user passwords. This includes, but is not limited to cracking, decoding, copying password files, "sniffing" packets for passwords or otherwise attempting to discover passwords belonging to other individuals;

- Logon/Operator IDs are only used by the person to whom they were assigned;

- Logon/operator IDs and passwords are not shared;

- Authorized user passwords are changed periodically;

- Passwords are kept confidential and secure. Passwords should not be stored in batch files, in automatic login scripts, in terminal function keys, in computers without access control or in other locations where another person might discover them;

- Authorized user passwords are not to be sent through electronic mail;

- All computer access granted to an authorized user will be removed when they transfer or terminate employment, graduate or withdraw from the University, or when a "courtesy account" is inactive or no longer needed. Files of transferred or terminated employees will be reviewed and disposed of by the appropriate manager in a timely and effective manner.

IV. COMPUTER AND SOFTWARE USAGE

Campus procedures regarding computer security and usage shall require that:

- University's computer systems are used for purposes related to 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;

- Authorized users use computing resources for the purposes related to their studies, their instruction, the performance of duties by an employee, or other University sanctioned activities. Use of the computing resources for commercial purposes not related to the University missions is prohibited;

- Abuse of the networks or of computers at other sites connected to the University's computers or networks by authorized users are treated as abuse of computing resources at the University;

- Any network traffic exiting the University system is subject to the acceptable use policy/guidelines of the network through which it flows, as well as the guidelines noted herein. Note that the laws of other states may apply depending on the actual location of the computer to which the authorized user

is networked (e.g., If you have connected to a computer in California, California computing laws must be adhered to. You can be prosecuted in any state through which your access flows or in which it terminates.);

- Possible loopholes in computer security systems are not be used to damage computer systems, obtain extra resources, take resources from another user, or gain access to any University computer system or any computer system networked to the University;

- Programs and files are confidential unless they have explicitly been made available to other authorized users. The University does not routinely examine files of authorized user accounts however, to protect the integrity of the computer systems and to protect legitimate users from the effects of unauthorized or improper use of the University's computing facilities, system/security administrators may inspect, copy, remove or otherwise alter any data, file or resource that may undermine the proper use of the computer system. Such action will be based on reasonable suspicion, authorized by the security administrator's supervisor and may be taken with or without notice to the user. Additionally, computer center personnel may access others' files when necessary for the maintenance of the computer system. When performing maintenance, every effort is made to insure the privacy and confidentiality of authorized user files;

- In an academic or instructional setting activities such as academic game development, computer security research, and the investigation of self-replicating code can be performed as long as authorized users involved in these activities contact the appropriate systems/security administrator so that the effects on the system can be determined and evaluated;

- The same standards of intellectual honesty and plagiarism apply to software as to other forms of published work. For example, individuals should not copy another's computer file and submit it as theirs nor should they work with someone else on an assignment, sharing the computer files and then submit that file, or a modification thereof, as their own individual work;

- Authorized users logoff University computer systems if they will not be accessing data for an extended time;

- Authorized Users understand and comply with their responsibilities as noted in the Responsibilities section of this document;

- Authorized users are aware that the University disclaims any loss or damage to software or data that results from its efforts to enforce these Guidelines.

VII. COMPLIANCE AND ENFORCEMENT

Campus procedures regarding computer security and usage should require that any individual found misusing University computing resources, accessing University computing resources without approval, or otherwise violating these Guidelines may be denied or given limited (i.e., to allow for the performance of required academic or employment related tasks) access to University computer systems and shall be subject to reprimand, suspension, dismissal, or other disciplinary action.

ATTACHMENT 1

University of Massachusetts
Computing Awareness and Data Security Compliance Statement

As an employee of the University of Massachusetts (the University) I understand that the unauthorized use or misuse of computer facilities, computer applications, computer systems, electronic mail and/or data constitutes an infraction of the University's policies/guidelines.

I recognize my individual responsibility for maintaining the confidentiality of data that I access while employed by the University as dictated by state and federal law, and University policy.

I will not improperly release any information obtained as a result of my position, nor will I compromise my right to access data by sharing or releasing any logon, operator id or password used to access University computer systems.

As an employee of the University I understand that I am entrusted with protecting the University's ownership and copyrights, and complying with University license agreements for software, equipment or data.

I recognize that the University licenses the use of commercial software and does not own this software or its related documentation or instructional material, and unless authorized by the software developer, does not have the right to copy computer software. I shall use software only according to the license agreement and shall use documentation only as allowed by the vendor and federal Copyright law.

I further acknowledge that University data, software or hardware should not be used in any commercial, illegal or unethical activities.

I have attended an orientation that included information regarding my computer security and data confidentiality responsibilities as an employee of the University. I understand these responsibilities both as an authorized user and an employee.

I recognize my overall responsibility to exercise the degree of care required to maintain control of University resources (e.g., data, software, hardware) and agree to abide by established University policies/guidelines and Campus procedures. I acknowledge that failure to comply with University computer and data related policies/guidelines/procedures may result in: the loss or restriction of my computer access; reprimand; suspension; dismissal, or other disciplinary action. Additionally, I understand that the University could also enforce its rights by the legal and equitable remedies to which it is entitled by law.

UNIVERSITY OF MASSACHUSETTS
DATA SECURITY AND CLASSIFICATION
(Doc. T97-010)

GUIDELINES

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 these systems be protected from misuse and that both the computer systems and all data be accessed and maintained in a secure environment. Data should be used responsibly and ethically.

I. PURPOSE

These Guidelines 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:

- outline responsibilities related to data security, signature imaging and documentation at the University of Massachusetts (the University);

- provide guidelines for the security, access and confidentiality of the University's data; and

- provide methods for monitoring and enforcing these Guidelines.

II. SCOPE

Campus procedures regarding data security and classification shall:

- 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 and confidentiality of data, including the Electronic Communications Privacy Act of 1986, Family Educational Rights and Privacy Act of 1974 (as amended), 20 U.S.C. 1232g, and the regulations promulgated thereunder, 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. Additionally, campus procedures may impose certain restrictions which 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;

- 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 authorized users of the University of Massachusetts;

- refer to all data as defined in the Definitions Addendum to these Guidelines.

Electronic mail message security and confidentiality are addressed in the University Electronic Mail Guidelines.

III. RESPONSIBILITIES

The President, together with the Chancellors, will issue guidelines which will:

- define what categories of individuals (e.g., full time, part-time, staff, students, economic partners, other educational institutions, general public, etc.) may access University data;

- determine what data are considered "institutional data" for the University.

The President shall appoint a Common Services central security specialist responsible for data and computer security planning, oversight, and coordination between campuses for centralized application systems and institutional data issues.

Campus procedures regarding data security and classification shall establish mechanisms to:

- determine which University department(s) shall be responsible for data security, which includes but is not limited to: monitoring and enforcing University/Campus data security policies, guidelines and procedures; coordinating or performing audits of data security; coordinating or performing incident investigations when a data security issue arises; and developing security awareness programs and training;

- appoint a campus central security specialist responsible for data and computer security planning, oversight, and coordination;

- appoint data custodians who are responsible for the day to day oversight of data as outlined below;

- determine which University department(s) shall be responsible for signature imaging records and documentation;

- assign data dissemination responsibilities.

Campus procedures regarding data security and classification shall require that central campus security specialists are responsible for:

- ensuring that audit trails exist for access and modification to Restricted and Confidential data, and other data as deemed appropriate;

- ensuring that a backup plan allowing for recovery of the data in the event of a disaster has been developed, tested and implemented;

- establishing when and ensuring that the level of risk to University data is assessed;

- ensuring that data are appropriately secured;

- reviewing and approving application systems changes which may affect the accessibility and security of the data;

- ensuring that a campus security awareness program has been developed and implemented.

Campus procedures regarding data security and classification shall require that data custodians are responsible for:

- knowing and understanding the data for which they are responsible;

- evaluating and ensuring the data has been appropriately classified based on: state and federal law, regulatory agency requirements and any contractual obligations; University policies/guidelines; and the confidentiality, criticality and sensitivity of the data;

- understanding the impact their design and access decisions have on the information and business needs of the users of the data. University policy may restrict or dictate the Data Custodian's role regarding data design and control (e.g., a policy indicating how access to Institutional Data should be handled would take precedent over individual Data Custodian decisions/determinations). Additionally, data custodians should make every attempt to support, not impede, University information and business needs;

- reviewing and approving application systems changes which may affect the accessibility and security of the data in their control, in conjunction with the central campus security specialist;

- determining, within any University policy/guidelines or Campus procedures, how data will be made available;

- ensuring that the accuracy of the data is maintained;

- determining and approving, within University policy/guidelines or Campus procedures, which individuals can access the data; ensuring that only these approved users have access to the data; and periodically reviewing whether any changes are needed;

- ensuring that all logon/operator IDs for individuals with access to University systems have been deleted when: an authorized user has terminated employment, graduated or withdrawn from the University, and when a "courtesy account" is inactive or no longer needed;

- designating, if needed, a security administrator(s) responsible for the day to day tasks related to data security (e.g., maintaining security access tables, developing security awareness training, etc.).

Campus procedures regarding data security and classification shall require that authorized users are responsible for:

- knowing and complying with University policies/guidelines, Campus procedures and application data security requirements;

- safeguarding the integrity, accuracy and confidentiality of University data as outlined in this or other University policies/guidelines, Campus procedures, or federal/state/local regulations;

- properly creating, accessing, using and disposing of University data based on the data's classification;

- backing up their personal/instructional data.

IV. DATA SECURITY

Campus standards regarding data security and classification shall require that:

- University data are protected in a manner which is commensurate with its classification and value;
- the cost of data security is commensurate with the classification and value of the data being secured;
- to the extent necessary, information is 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;
- Restricted and Confidential data contain audit trails to monitor access and modification, and is appropriately backed up to allow for recovery;
- University data, regardless of medium and/or form, will be disseminated by officially designated offices only,
- All job or course specific access granted to an authorized user will be removed when that user transfers from one department to another or when a course is completed. 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;
- Individuals observing data security violations should report such violations to the appropriate data custodian and, in the case of employees, their direct supervisor;
- If required by law or regulation, the University will promptly report data security violations to external authorities. If no such requirement exists, the President, together with the appropriate campus Chancellor(s) will weigh the pros and cons of external disclosure before reporting these violations. Representatives from University Counsel, University Audit, and security should assist University management in their determination of the pros and cons of disclosure.

V. DATA CLASSIFICATION

Campus standards regarding data security and classification shall require that University data classifications are adhered to. Five 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 thereunder, 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 is made available to data custodian approved users only.

- Private - 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.

- Restricted - data whose loss, corruption or unauthorized disclosure would tend to impair the business or research functions of the University, or result in any business, financial, or legal loss.

- Confidential - data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts.

Campus procedures regarding data security and classification shall require that data, regardless of medium and/or form, will be:

- identified as to its classification (i.e. Unclassified, Operational Use Only, Private, Restricted or Confidential);

- accessed, used and disposed of in a manner commensurate with the data's classification and with University Records Management, Disposition and Retention Polices/Guidelines/Schedules and Campus procedures;

- made secure against unauthorized creation, updating, processing, outputting, and distribution;

- appropriately secured and not accessible to non-approved users when not in use.

Campus procedures regarding data security and classification shall require that:

- 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).

- Databases containing Operational Use Only, Private, Restricted or Confidential data should be secured. Extracts of Operational, Private, Restricted or Confidential data should be secured at the same level as the file/database from which the data was extracted.

- Reports containing Operational Use Only, Private, Restricted 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.

VI. DATA ACCESS AND USE

Undefined or unclear guidelines or procedures shall not be construed to imply access authorization.

Campus procedures regarding data security and classification shall require that:

- only authorized users have access to University data;
- access to data other than unclassified data is denied unless the user has obtained explicit approval by the data custodian;
- access to data classified as Private, Restricted or Confidential should be based on legal requirements or on a need to know; job function; or course requirement basis;
- access to data is given to authorized users. This access should not be shared, transferred or delegated (e.g., authorized users should not log on, access data and then let others use that data);
- vendors, contractors, consultants and external auditors needing access to University data have read, and acknowledge in writing that their firm has read, understood and will comply with the University Data Security and Classification Guidelines and Campus procedures;
- authorized users act in a manner which will ensure the data they are authorized to access is protected from unauthorized access, unauthorized use, invalid changes (e.g., putting a Q in a grade field), destruction, or improper dissemination;
- authorized users will use their access to University data for approved purposes only;
- authorized users logoff University computer systems if they will not be accessing data for an extended time;
- authorized users will not use University applications and their data in illegal activities;
- authorized users are prohibited from viewing or accessing data, in any medium and/or form, for which they are not approved;
- classified data are not copied without prior approval;
- authorized users understand the data they are accessing and the level of protection required;
- authorized users set file protections correctly when they create or copy a file;
- authorized users periodically "refresh" downloaded data to ensure they are working with accurate, up-to-date data.

VII. SIGNATURE IMAGING

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.

Each new use of any electronic authorization process or signature imaging within a computer application must be approved by the Chancellor of the campus instituting the new procedure.

The system controls for each new electronic authorization process or signature imaging are subject to review by the University Auditor's Office.

When signature imaging is used, campus procedures should require that:

- A signature card with the employee's/student's handwritten signature and access authorizations for any individual using signature imaging will be centrally maintained at each campus.

- An electronic record of each signature and document must be retained for a minimum of seven years, unless an alternate time period is specified by law or other university policy.

VIII. COMPLIANCE AND ENFORCEMENT

Campus procedures regarding data security and classification should require that any individual found misusing data, divulging confidential data or otherwise violating these Guidelines may be denied or given limited (i.e., to allow for the performance of required academic or employment related tasks) access to data and/or University computer systems, and shall be subject to reprimand, suspension, dismissal, or other disciplinary action.

UNIVERSITY OF MASSACHUSETTS
ELECTRONIC MAIL GUIDELINES
(Doc. T97-010)

GUIDELINES

The University works in a large, complex information technology environment requiring communication related to both confidential and public data. New technologies offer the University methods to make this communication easier between students, staff, departments, campuses, colleges, and the world. The University has several types of electronic mail systems on its various computer systems enabling its students and employees to take advantage of these technologies. However, with this open communication network, vulnerabilities to the privacy of electronic messages possibly containing confidential or proprietary material arise. University electronic mail users need to be aware of the vulnerabilities in electronic mail communication and of the legal responsibilities that accompany the use of this medium.

I. PURPOSE

These Guidelines 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:

- define who may use the electronic mail systems controlled and administered by the University of Massachusetts (the University);
- outline responsibilities related to electronic mail maintenance and use;
- provide guidelines for the security and confidentiality of University electronic mail; and
- provide methods for monitoring and enforcing these Guidelines.

II. SCOPE

Campus procedures relating to electronic mail shall apply to all:

- electronic mail (e-mail) created within, sent to, maintained within, or administered by the electronic mail systems of the University of Massachusetts;
- University e-mail users;
- electronic mail as defined in the Definitions Addendum to these Guidelines.

III. RESPONSIBILITIES

The President, together with the Chancellors, shall define what categories of individuals (e.g., full time, part-time, staff, students, economic partners, other educational institutions, general public, etc.) may access University electronic mail systems.

The Chancellors, or their designees, will determine:

- which University department(s) shall be responsible for administering electronic mail systems and security;

- procedures for electronic mail monitoring related to Section V, Items D and E of these Guidelines.

Campus procedures relating to electronic mail will require that 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 a backup plan to allow for message/system recovery in the event of a disaster has been developed, tested and implemented;

- ensuring that **deleted and expired** mail 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;

- periodically assessing the level of risk within the mail system;

- 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 all electronic mail IDs for individuals with e-mail accounts on University systems have been deleted when: an authorized user has terminated employment, graduated or withdrawn from the University, and when a "courtesy account" is inactive or no longer needed;

- 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.

Campus procedures relating to electronic mail will require that employees responsible for maintaining, repairing and developing e-mail resources 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.

Campus procedures relating to electronic mail will require that University E-mail Users:

- use e-mail in a responsible manner consistent with other business communications (e.g., phone, correspondence);

- safeguard the integrity and confidentiality of University electronic mail;

- only use mail IDs assigned to them;

- remove mail from their mailbox consistent with University, campus, departmental or electronic mail administrator message retention procedures and these Guidelines.

Campus procedures relating to electronic mail will require that University e-mail users NOT:

- post materials that violate existing laws or University policies/codes of conduct. For example, materials that are of a fraudulent, defamatory, harassing, or threatening nature;

- use their e-mail access to unlawfully solicit or exchange copies of copyrighted software.

IV. ELECTRONIC MAIL USE GUIDELINES

Campus procedures relating to electronic mail will require that:

- Individuals are prohibited from using an electronic mail account assigned to another individual to either send or receive messages. If it is necessary to read another individual's mail (e.g., while they are on vacation, on leave, etc.), surrogacy or message forwarding should be utilized.

- The University makes e-mail facilities available to both students and staff. University E-Mail Users are encouraged to use these communications resources to share knowledge and information in furtherance of the University's missions of instruction, research, and public service. Students are free to use e-mail for personal use. E-mail is made available to employees for the purpose of conducting University-related business, but occasional social/personal use is allowed providing it does not interfere with an employee's job function.

- Individuals with e-mail IDs on University computer systems are prohibited from sending messages which violate state or federal law, or University policy. 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.

- Authorized users will not "rebroadcast" information obtained from another individual that the individual reasonably expects to be confidential.

- Bulletin Boards used for soliciting or exchanging copies of copyrighted software are not permitted on University electronic mail systems.

- Authorized users are prohibited from sending, posting or, publicly displaying or printing unsolicited mail or materials that are of a fraudulent, defamatory, harassing, abusive, obscene or threatening nature on any University system. The sending of such messages/materials will be handled according to University codes of conduct, policies and procedures.

- The University can not control the content of electronic mail. If an individual receives electronic mail that they consider harassing, threatening or offensive, they should contact the appropriate University Office for assistance.

V. ELECTRONIC MAIL INFORMATION

Campus procedures relating to electronic mail will require that e-mail users are aware and understand that:

- The University considers a personal e-mail message to be private correspondence within the limits set forth in this section, but due to the nature of the electronic medium the University cannot guarantee the privacy or security of such correspondence and e-mail users are cautioned that such messages might become available to others.

- The University considers electronic mail messages (other than such correspondence which might constitute public records) to be the property of the sender and receiver. However, since the messages are stored on University computer systems, the University has responsibility for the administration of the electronic mail systems.

- The University will not routinely monitor the content of electronic documents or messages, however, the privacy of documents and messages stored in electronic media cannot be guaranteed. Electronic documents and messages may be readable to maintenance, security and troubleshooting staff while performing their job functions. Such access will occur only when a problem in the software or network arises. Additionally electronic mail may pass out of one computer environment, across a network, and into another totally different computer environment even within the University system. This transport becomes increasingly complicated as mail travels between departments, campuses, universities, states, or nations. The level of security over a message is affected each time the computer hardware, software and environment changes. Untraceable leaks may occur.

- If there is a University investigation for alleged misconduct, the Chancellor or their designee may authorize that electronic mail or files may be locked or copied to prevent destruction and loss of information.

- The University may monitor the content of electronic documents and messages, or access e-mail backups or archives as a result of legal discovery, writ, warrant, subpoena, or when there is a threat to the computer system's integrity or security as determined by the system administrator.

- The confidentiality of the contents of e-mail messages that include certain types of information (e.g., student related, medical, personal) may be protected by the Family Educational Rights and Privacy Act of 1974 (as amended), the Electronic Communications Privacy Act of 1986, or other state or federal law. Additionally the contents of e-mail messages may be classified as public by the Massachusetts Fair Information Practices Act (M.G.L. c66A) and/or the Massachusetts Public Records Act (M.G.L. c66), section 10.

- The authenticity of an e-mail message cannot be assured due to the state of present e-mail technology. This means that the authorship or source of an e-mail message may not be as indicated in the message.

VI. COMPLIANCE AND ENFORCEMENT

Campus procedures regarding electronic mail will require that any individual found breaching the confidentiality of e-mail messages, disclosing confidential University data by using e-mail, or otherwise violating these Guidelines, may be denied or given limited (i.e., to allow for the performance of required

academic or employment related tasks) access to the e-mail and/or University computer systems, and shall be subject to reprimand, suspension, dismissal, or other disciplinary action.

UNIVERSITY OF MASSACHUSETTS

DEFINITIONS ADDENDUM

- Computer Security and Usage Guidelines
- Data Security and Classification Guidelines
- Electronic Mail Guidelines

Academic Computing refers to computer systems that support the research and educational mission of the University.

Administrative Computing refers to computer systems that support the operational functions (e.g., financial, payroll/personnel, library, and student related data such as major, grades, courses, etc.) of the University.

Anonymous Connection is the act of connecting to a remote computer as an unidentified or anonymous user.

Approved Users Authorized Users who have been given explicit access to specific data by the Data Custodian.

Audit Trail is a log(s) of specified access (e.g., when, how, from where and by whom data is accessed). For example, a log of all changes to student grades would be kept to monitor who was accessing such confidential data and what they were doing (e.g., reading, updating, deleting).

Authorized Users are all students and employees (including student, non-student, faculty, professional, classified, temporary, part-time, and full-time), and contracted consultants of the University of Massachusetts who are required to have access to data to perform their job function, academic assignment, or contractual obligations. Authorized users also include those individuals who are assigned courtesy accounts.

A Bulletin Board/Newsgroup is a service that enables users to post information for or seek information from others who are interested in a certain topic(s).

Campus or University Computing Infrastructure refers to the underlying technology (e.g., hardware, cabling, telecommunications and software) required to support the primary University/Campus computing and data communications environments which are usually maintained by computing centers. This does NOT include departmental computing resources (e.g., a department level computing system or network).

Campus Procedures are statements designed to comply with the requirements of University Guidelines by establishing specific criteria that must be met by University students, staff, consultants, etc.

Central Security Specialist is an individual(s) at each campus and the President's Office who has experience, knowledge and understanding of information systems security practices/requirements and who is responsible for data and computer security planning, oversight, and coordination.

Classified Data refers to University data which has been identified as Operational, Private, Restricted or Confidential.

Computer Applications are sets of computer programs which when run read or modify data, and which can generate output such as reports, bills, checks, etc.

Computer Security refers to the development and implementation of a system of controls which when implemented will REDUCE the PROBABILITY of something negative occurring (e.g., unauthorized file access or modification). Computer Security includes the following categories of control: Administrative (e.g., polices/procedures, personnel, and contingency planning); Hardware; Software (e.g., operating and application system software); Data; Communications/ Network; Physical and Environmental; Legal (e.g., state, federal & regulatory).

Computer System(s) refers to the hardware, software and communications equipment used in the processing and storage of electronic data.

Confidential Data is University data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts.

Courtesy Accounts are accounts on University computer systems which may be provided to individuals who are not University employees, students, or contracted consultants but who have an established relationship with the University and need access. Examples include alumni, business partnerships, individuals from other educational institutions, etc.

Data refers to information regardless of the medium on which it resides (i.e., tape, cartridge, disk, hard drive, etc.), and regardless of its form (e.g. text, graphic, video, voice, etc.).

Data Integrity refers to the completeness and accuracy of data.

Data or Information Security shall mean the implementation of reasonable safeguards to prevent unauthorized access, theft, removal or misuse of University electronic data (i.e., tape, cartridge, disk, hard drive, etc.).

Data Custodian(s) are the individual(s) responsible for making decisions about the sensitivity and critically of specific University systems and data stored in these systems; determining the classification of data under their control; documenting the use of the specific system(s); and determining which University staff require access to that system and its data. University policy may restrict or dictate the Data Custodian's role regarding data design and control (e.g., a policy indicating how access to Institutional Data should be handled would take precedent over individual Data Custodian decisions/determinations). Examples of Data Custodians are: the Directors of Human Resources would have Data Custodian responsibility over payroll and personnel information and a Principal Investigator is the Data Custodian for research data related to their grant.

Degree of Risk or Levels of Risk refer to the amount of exposure and/or vulnerability associated with a particular entity such as a computer system. Examples of exposure or vulnerability include theft; unauthorized access; unauthorized alternation or destruction of the computer system or the data stored on it; human error; natural disasters, etc.

Deleted E-Mail refers to any e-mail which an e-mail users has specifically deleted/removed from their e-mail mailbox or electronic mail files.

Electronic Mail (e-mail) refers to letters, files and messages sent by one computer user or a software agent to a specific user or set of users within the same computer system or over a computer network.

Electronic Mail Id is a unique code which identifies a specific person to an electronic mail system.

An Electronic Mail Administrator is the individual responsible for making decisions about how an electronic mail system(s) should be maintained, determining classes of individuals which may use the electronic mail system, and determining how the mail system and its capabilities will be implemented and secured.

An Electronic Mail System is a computer which has e-mail capabilities on it.

Electronic Signature is the method of ensuring that the purported signer of a document was the actual signer and the document has not been modified since signed.

Employees are all student, non-student (faculty, professional, classified), temporary, part-time, full-time, contracted and consultants who are paid from University funds and require access to electronic data to perform their job function.

External E-mail Users are individuals who communicate with University mail systems from mail systems not controlled or administered by the University (e.g., Internet).

A Filter is a security method to "hide" e-mail message text from the view of electronic mail maintenance personnel.

Idle Time or Time-Out refers to a capability within computer systems to disconnect an authorized user if that user is logged on and has not communicated with the computer for a specified period of time (i.e., 15 minutes).

Internet is a network of computers that allows its users to send mail or access data world-wide.

Levels of Risk or Degree of Risk refer to the amount of exposure and/or vulnerability associated with a particular entity such as a computer system. Examples of exposure or vulnerability include theft; unauthorized access; unauthorized alternation or destruction of the computer system or the data stored on it; human error; natural disasters, etc.

Licensed Software is software that has been developed for commercial "sale" or for limited/restricted use. The software developer maintains copyright to the software and sells others the right to use the software for a fee. Note that the developer retains ownership of the software and controls how the software can be used.

A Logon or Operator Id is a unique code that identifies a specific person to the computer system. A Logon or Operator Id may also identify a type of user (i.e., Internet) to the computer system.

Mailbox is the area in the computer in which e-mail users receive electronic mail messages.

Message Encryption is the scrambling of e-mail messages so they are more secure and not easily read by anyone other than the designated recipient who has been given the "key" to unscramble the message.

Operational Use Only Data University data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss BUT which is made available to Data Custodian approved users only.

Packet refers to a "bundle" of information sent over network. Packets usually include information regarding where the data is being sent, the actual data, and a record indicating the end of the packet.

Packet Sniffing is a technique in which an individual inserts a software program at remote network switches or computers for the purpose of monitoring information sent over the network.

A Password is a confidential, unique code used in conjunction with the logon id to verify that the user trying to access the computer is the person to whom the Logon/Operator ID was assigned.

Password Creation Checking is the process of a computer system comparing a user's password to words in a dictionary; user specific data such as logon id, name, birth date, social security number; and common character sequences such as "123456" or "abcdef".

Private Data is 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.

Protocol is a set of formats and procedures governing the exchange of information between computer systems.

Public Domain Software is software for which the titles and copyrights have been explicitly relinquished by the author, so that anyone can use it as they please, free of charge.

Rebroadcast is to transmit or make information accessible to individuals not materially involved in the issue that the information relates to (e.g. posting the information to a newsgroup, emailing it to others, or creating a link to the information from a publicly available Web page).

Research Computers are any University computers which contains data related to faculty/staff/student research. This does not include the accounting data related to the financial functions of a research grant.

Restricted Data is University data whose loss, corruption or unauthorized disclosure would tend to impair the business or research functions of the University, or result in any business, financial, or legal loss.

Retention Standards are requirements which indicate the period of time a type of data or message should be retrievable.

Secured Data refers to data that is available to authorized users who require this access to perform their job function and who have obtained Data Custodian approval for this access.

Server refers to computers that provide resources or information to other computers. There are many types of servers including file servers, terminal servers, and name servers.

Shareware refers to copyrighted software whose license allows the software to be freely copied and shared. The use of Shareware usually requires the payment of a fee after some time period specified in the software's license.

Signature Images refer to the entry of a signature on a computerized document by electronic means.

Staff refers to all non-student (faculty, professional, classified), temporary, part-time, full-time, contracted and consultants who are paid from University funds and require access to electronic data to perform their job function.

Students are all individuals enrolled at the University of Massachusetts and its programs. This includes individuals attending day, continuing education, graduate and/or undergraduate sessions who may be part-time or full-time students. (NOTE: While performing job functions related to student employment with the University, students are considered employees and must therefore abide by employee related policies.)

Student Data refers to data that is created by University students.

Surrogacy refers to a situation in which an authorized e-mail user has given another authorized e-mail user permission to access certain features of their mail account. The surrogate uses their own mail id to access the other users mail features, they DO NOT use the other users mail id. For example, a Department Head or Director may give their assistant surrogate access to their mailbox so that the assistant may screen the Department Head's or Director's mail. The assistant would access the mail system using their own electronic mail id but would be able to view the Department Head's/Director's mail.

A Third Party is any individual, group of individuals, bulletin board, conference or newsgroup either within the University or at any other location world wide who is not originally addressed in the e-mail message.

Third Party Data is any data supplied by and/or maintained for a Third Party.

Time-Out or Idle Time refers to a capability within computer systems to disconnect an authorized user if that user is logged on and has not communicated with the computer for a specified period of time (i.e., 15 minutes).

Trojan Horse, Virus, or Worm is computer code designed to self-replicate, damage, or otherwise hinder the performance of a computer's memory, file system, or software.

Unauthorized User is any individual accessing data which is other than non-classified to which they have not been given explicit approval by a Data Custodian.

Unclassified Data is University data that does not fall into any of the other data classifications (i.e., Operational, Private, Restricted or Confidential). This data maybe made generally available without specific Data Custodian approval.

University Data is data created, executed or received by an University employee (i.e., full or part time, temporary, professional, classified or faculty) in connection with the transaction of University business. Categories of University data are Financial, General, Medical, Personnel, Student, etc.

University E-mail Users are all individuals who have accounts on electronic mail systems under the control and administration of the University of Massachusetts.

University or Campus Computing Infrastructure refers to the underlying technology (e.g., hardware, cabling, telecommunications and software) required to support the primary University/Campus computing and data communications environments which are usually maintained by computing centers.

This does NOT include departmental computing resources (e.g., a department level computing system or network).

University Guidelines are statements designed to achieve the requirements of University Policies by establishing specific criteria that must be met in Campus Procedures.

University Policies are concise statements of direction and required action issued only by the Board of Trustees.

Virus, Worm or Trojan Horse is computer code designed to self-replicate, damage, or otherwise hinder the performance of a computer's memory, file system, or software.

Web Page refers to a page of information available on the World-Wide web network.

World-Wide Web is a distributed information system that can be accessed to retrieve data in text, video or audio format.

Worm, Virus or Trojan Horse is computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software.