UNIVERSITY OF MASSACHUSETTS BOSTON

POLICIES AND PROCEDURES

I have received, read, understood and acknowledge my responsibility to conduct myself consistent with University and Commonwealth policies, including but not limited to those attached:

- Data Security, Electronic Mail and Computer Policy Development (Doc. T97-010)
- Drug-Free Workplace Policy
- Federal Affordable Care Act (ACA) notification/information
- Guide to the Conflict of Interest Law
- Guide to Political Activity (Public Employees and Fundraising)
- Massachusetts Pregnant Workers Fairness Act
- Non-Discrimination and Harassment Policy (Doc. T16-040)
- Sexual Harassment Policy (Doc.T92-037)
- University of Massachusetts Boston Background Check Policy
- University of Massachusetts Policy on Fraudulent Financial Activities (Doc. T00-051)
- University of Massachusetts Principles of Employee Conduct (Doc. T96-136)

DEPARTMENT OF HUMAN RESOURCES
UNIVERSITY OF MASSACHUSETTS BOSTON
100 MORRISSEY BLVD
BOSTON, MA 02125-3393
617-287-5150 (MAIN)
617-287-5179 (FAX)
WWW.HR.UMB.EDU/POLICIES

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.

UMASS BOSTON
UNIVERSITY OF MASSACHUSETTS BOSTON
HUMAN RESOURCES

100 Morrissey Boulevard
Boston, MA 02125-3393
P: 617.287.5150
F: 617.287.5179
www.umb.edu/hr

POLICY & GUIDANCE MEMORANDUM

#2009-16: Drug-Free Workplace

University policy requires that the following notice be distributed each year throughout the UMass Boston community.

The University of Massachusetts Boston, in accordance with both federal legislation and existing University policy, is committed to providing a drug-free, healthful, and safe environment for all employees.

In the event that an employee is observed to be under the influence of drugs or alcohol during work hours, appropriate disciplinary action is to be taken. The progression of actions, from the least to the most severe, is the following:

1. The immediate supervisor will discuss his/her concerns and observations with the employee. He/she will recommend that the employee seek professional assistance and will suggest a referral to a substance abuse counseling/rehabilitation program. This will occur on an informal (verbal) basis and will not be included in the employee's personnel record. Appropriate arrangements will be made to ensure that the employee reaches his/her home safely that day.

2. Should there be a repeat occurrence, a formal written warning will be given, and again, the employee will be encouraged to utilize the services of a counseling/rehabilitation program.

3. Any continued use by the employee of drugs and/or alcohol at work will result in a suspension from work ranging from one to five days. At this time, the employee will be required to utilize the services of a counseling/rehabilitation program as a condition of employment.

4. Further use in the workplace of drugs and/or alcohol or failure to utilize the services of a counseling/rehabilitation program will result in a longer suspension and/or termination.

All employees will have available the appropriate hearing and grievance procedures during these disciplinary actions.

In addition, under the terms of the Drug Free Workplace Act, any employee engaged in the performance of a federal grant must, as a condition of employment, notify the employer of any criminal drug statute conviction for a violation occurring in the workplace no later than five days after such a conviction.

Upon notification by an employee the University must, within 30 (thirty) days of receiving such notification with respect to any employee who is so convicted:(1) Take appropriate

personnel action against such an employee, up to and including termination, or (2) Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program.

The University recognizes alcohol and drug dependency as an illness and a major health problem. Alcohol is the number one drug problem in the country. Drinking alcohol has acute effects on the body. It impairs judgment, vision, coordination and speech and often leads to dangerous risk-taking behavior. These may include drunken driving, injuries and serious accidents. Nearly half of all accidental deaths, suicides and homicides are alcohol related. The misuse of alcohol is often involved in violent behavior, acquaintance rape, unintended pregnancies, and the exposure to sexually transmitted diseases. Long-term excessive drinking and drug use can lead to a wide variety of health problems in many different organ systems.

The use of drugs and alcohol can cause physical and psychological dependence. They can interfere with memory, sensation and perception. Drugs impair the brain's ability to synthesize information. Regular users of drugs develop tolerance and physical dependence often experienced by withdrawal symptoms. The psychological dependence occurs when the drug taking becomes central to the user's life.

Finding Help for Alcohol and Other Drug Problems (See Appendix A)

Many people with alcohol or other drug problems can be treated successfully entirely on an outpatient basis and do not have to interrupt their work and home lives. Outpatient programs exist in a variety of settings, including community mental health centers, family service agencies, private physicians' and therapists' offices, and specialized treatment facilities. Inpatient services, designed for those with more serious alcohol problems, can be found in hospitals, residential care facilities and community half-way houses.

Paying for Treatment

If you are covered by an insurance plan through the Group Insurance Commission, your insurance will pay for a portion of treatment for alcohol or other drug problems. Each plan has different provisions, but all provide some level of coverage. Contact your plan for information as to how you access treatment.

Employee Assistance Program

UMass Boston is pleased to offer ComPsych Guidance Resources to all of its employees. ComPsych is a comprehensive employee assistance program that provides confidential consultants you can call on the phone 24/7.

The EAP is a practical, confidential and constructive mechanism for dealing with employees' personal problems that may affect the work situation, or as an aid to those employees and their family members who wish to use the program as a means of resolving a personal problem.

The purpose of the Employee Assistance Program is to provide assistance to employees who are dealing with personal difficulties such as emotional problems, substance abuse issues,

relationship and family crises, and legal and financial concerns. Almost any personal or family problem can be successfully treated provided it is identified in its early stages and referral is made to an appropriate professional. This applies whether the problem is one of physical, mental or emotional illness, finances, etc.

To contact ComPsych, call 844-393-4893 or visit ComPsych online at www.guidanceresources.com (company ID: UMASS). For TDD service, call 800-697-0353. For additional information about how to use the program, contact the Department of Human Resources at 617-287-5150.

Summary of Massachusetts Substance Abuse Laws

• Massachusetts law prohibits the sale or delivery of alcoholic beverages to persons under 21 years of age, with a fine of up to $2,000 and 1 year imprisonment, or both, for violations. Misrepresenting one's age or falsifying an identification to obtain alcoholic beverages is punishable by a fine of $200 and up to 3 months imprisonment.

• A first conviction for driving under the influence of alcohol has a penalty of a $500 up to $5,000 fine, a revocation of one's driver's license, up to two½ years in prison, and mandatory participation in an alcohol rehabilitation program.

• Cities and towns in Massachusetts prohibit public consumption of alcohol and impose fines for violations. The Metropolitan District Commission also prohibits public consumption of alcohol in its parks.

• Criminal penalties for the illicit use of controlled substances ("drugs") vary with the type of drug. In general, narcotics, addictive drugs, and drugs with a high potential for abuse, have heavier penalties.

• Possession of controlled substances is illegal without valid authorization. While penalties for possession are generally not as great as for manufacture and distribution of drugs, possession of a relatively large quantity may be considered distribution. Under both State and Federal laws, penalties for possession, manufacture and distribution are much greater for second and subsequent convictions. Many of these laws dictate mandatory prison terms and require that the full minimum term be served.

• Massachusetts law makes it illegal to be in a place where heroin is kept and to be "in the company" of a person known to possess heroin. Anyone in the presence of heroin at a private party risks a serious drug conviction. Sale and possession of "drug paraphernalia" is also illegal in Massachusetts.

• It is illegal in Massachusetts to aid or abet a person under the age of 18 in dispensing, distributing or possessing with the intent to distribute or sell a controlled substance. Conviction leads to a minimum term of five years in prison.

Federal Penalties and Sanctions for Illegal Possession of a Controlled Substance

• 21 U.S.C. 844(a)
1st conviction: Up to 1 year imprisonment and fined at least $1,000 but no more than $100,000, or both.

After 1 prior drug conviction: At least 15 days in prison, not to exceed 2 years and fined at least $2,500

After 2 or more prior drug convictions: At least 90 days in prison, not to exceed 3 years and fined at least $5,000 but no more than $250,000, or both.

Special sentencing provision for possession of crack cocaine: Mandatory at least 5 years in prison, not to exceed 20 years and fined up to $250,000, or both, if:

(a) st conviction and the amount of crack possessed exceeds 5 grams.
(b) 2nd crack conviction and the amount of crack possessed exceeds 3 grams.
(c) rd or subsequent crack conviction and the amount of crack possessed exceeds 1 gram.

• 21 U.S.C. 853(a)(2) and 881 (a)(7)
Forfeiture of personal and real property used to possess or to facilitate possession of a controlled substance if that offense is punishable by more than 1 year imprisonment. (See special sentencing provisions re: crack)

• 21 U.S.C. 881(a)(4)
Forfeiture of vehicles, boats, aircraft or any other conveyance used to transport or conceal a controlled substance.

• 21 U.S.C. 844a
civil fine of up to $10,000 (pending adoption of final regulations.)

• 21 U.S.C. 853a
Denial of Federal benefits, such as student loans, grants, contracts, and professional commercial licenses, up to 1 year for the first offense, up to 5 years for second and subsequent offenses.

• 18 U.S.C. 922(g)
Ineligible to receive or purchase a firearm.

• Miscellaneous
Revocation of certain Federal licenses and benefits, e.g., pilot licenses, public housing tenancy, etc., are vested within the authorities of individual Federal agencies

Appendix A

Alcohol and Drug Help Resources

This is only a partial listing of many available treatment and recovery resources.

Counseling Center staff can assist students concerned about their use of alcohol or other drugs. Help is also available to students who are concerned with or affected by the use/abuse of alcohol or other drugs by a family member, friend, or roommate. Call 508-999-8650.

Counseling Center can also assist faculty, staff, and students in locating resources that are best suited to meet their needs. Call 508-999-8650.

Massachusetts Substance Abuse Information and Education Helpline
1-800-327-5050
<http://www.helpline-online.com/>www.helpline-online.com
The Helpline provides consumers with comprehensive, accurate, and current information about alcohol and drug treatment and prevention services throughout Massachusetts. Free and confidential. 24/7.

Substance Abuse Treatment Facility Locator
1-800-622-HELP
<http://www.findtreatment.samhsa.gov/>www.findtreatment.samhsa.gov
A searchable directory of drug and alcohol treatment programs shows the location of facilities around the country that treat alcoholism, alcohol abuse, and drug abuse problems.

Alcoholics Anonymous World Services
<http://www.alcoholics-anonymous.org/>www.alcoholics-anonymous.org
Alcoholics Anonymous is a voluntary, worldwide fellowship of men and women who meet together to attain and maintain sobriety through a 12-step program. Visit this site for more information and a searchable directory of offices in U.S. and Canada. Contact the office closest to your address for support group meeting locations and times.

Al-Anon Family Groups
1-888-425-2666
<http://www.al-anon.alateen.org/>www.al-anon.alateen.org
www.ma-al-anon-alateen.org (Massachusetts Al-Anon Alateen Web Site)
The two branches of the Al-Anon Family Groups include Al-Anon and Alateen, serving adults and teens who are relatives and friends of alcoholics. Visit this site for more information and a searchable directory of offices in U.S. and Canada. Contact the office closest to your address for support group meeting locations and times.

Narcotics Anonymous
<http://www.na.org/>www.na.org
www.newenglandna.org (New England Region of N.A.- Serving Eastern Mass. & R.I.) 1-866-624-3578 (New England Region of N.A.-Serving Eastern Mass. & R.I.)

Narcotics Anonymous is an international, community-based association of recovering drug addicts with more than 33,500 weekly meetings in over 116 countries worldwide. Visit the New England Region of Narcotics Anonymous website for regional support group meeting times and locations.

Nar-Anon Family Groups
1-800-477-6291
<http://www.nar-anon.org/>www.nar-anon.org
Nar-Anon serves adults and teens who are relatives and friends of someone with a drug problem or addiction. Visit this site for more information and a searchable directory of support groups in the U.S. and abroad.

Marijuana Anonymous
1-800-766-6779
<http://www.marijuana-anonymous.org/>www.marijuana-anonymous.org
Marijuana Anonymous is a fellowship of men and women who meet together to recover from marijuana addiction through a 12-step program modeled upon that of Alcoholic Anonymous. Call 1-800-766-6779 for support group meeting times and locations or visit www.ma-online.org for online meeting support.

Alcohol and Drug Informational/Educational Resources

This is only a partial listing of many available educational and informational resources. Health Education staff can assist faculty, staff, and students in locating resources that are best suited to meet their needs. Call 508-910-6965.

National Clearinghouse for Alcohol & Drug Information
<http://www.health.org/>www.health.org
1-800-729-6686

National Institute on Drug Abuse
<http://www.drugabuse.gov/>www.drugabuse.gov

Facts on Tap
<http://www.factsontap.org/>www.factsontap.org
1-800-488-DRUG (3784)
Alcohol and drug education, prevention, intervention for college students. Information for college students, their parents, and campus professionals.

MyStudentBody
<http://www.mystudentbody.com/>www.mystudentbody.com
Reliable health information on alcohol, tobacco, and sexually transmitted diseases, customized for college students.
Faculty and staff: Wish to access MyStudentBody.com? Contact the Health Education Office at 508-910-6965 for a code to enter the site.

Go Ask Alice!
<http://www.goaskalice.com/>www.goaskalice.com
Go Ask Alice! is Columbia University's leading health question and answer service with an archive of over 2,500 straight-forward and in-depth responses to questions sent anonymously.

College Drinking Prevention (National Institute on Alcohol Abuse & Alcoholism)
<http://www.collegedrinkingprevention.gov/>www.collegedrinkingprevention.gov
Information on college drinking and prevention for campus professionals, community leaders, high school guidance counselors

Overview of Health Insurance Marketplaces

HEALTH CONNECTOR
the right place for the right plan

YOU ARE RECEIVING THIS NOTICE AS REQUIRED BY THE NEW NATIONAL HEALTH REFORM LAW (ALSO KNOWN AS THE AFFORDABLE CARE ACT OR ACA)

On January 1, 2014, the Affordable Care Act (ACA) will be implemented in Massachusetts and across the nation. The ACA will bring many benefits to Massachusetts and its residents, helping us expand coverage to more Massachusetts residents, making it more affordable for small businesses to offer their employees healthcare, and providing additional tools to help families, individuals and businesses find affordable coverage. This notice is meant to help you understand health insurance Marketplaces, which are required by the ACA to make it easier for consumers to compare health insurance plans and enroll in coverage. In Massachusetts, the state Marketplace is known as the Massachusetts Health Connector. While you may or may not qualify for health insurance through the Health Connector, it may still be helpful for you to read and understand the information included here.

Overview: When key parts of the national health reform law take effect in January 2014, there will be an easy way for many individuals and small businesses in Massachusetts to buy health insurance: the Massachusetts Health Connector. This notice provides some basic information about the Health Connector, and how coverage available through the Health Connector relates to any coverage that may be offered by your employer. You can find out more by visiting: **MAhealthconnector.org**, or for non-Massachusetts residents, **Healthcare.gov** or (1-800-318-2596; TTY: 1-855-889-4325).

What is the Massachusetts Health Connector? The Health Connector is our state's health insurance Marketplace. It is designed to help individuals, families, and small businesses find health insurance that meets their needs and fits their budget. The Health Connector offers "one-stop shopping" to easily find and compare private health insurance options from the state's leading health and dental insurance companies. Some individuals and families may also qualify for a new kind of tax credit that lowers their monthly premium right away, as well as cost sharing reductions that can lower out-of-pocket expenses. This new tax credit is enabled by §26B of the Internal Revenue Service (IRS) Code.

Open enrollment for individuals and families to buy health insurance coverage through the Health Connector begins Oct. 1, 2013, for coverage starting as early as Jan. 1, 2014. (And in future years, open enrollment will begin every Oct. 15.) You can find out more by visiting **MAhealthconnector.org** or calling **1-877-MA ENROLL** (1-877-623-6765).

Can I qualify for federal and state assistance that reduces my health insurance premiums and out-of-pocket expenses through the Health Connector?

Depending on your income, you may qualify for federal and/or state tax credits and other subsidies that reduce your premiums and lower your out-of-pocket expenses if you shop through the Health Connector. You can find out more about the income criteria for qualifying for these subsidies by visiting **MAhealthconnector.org** or calling **1-877-MA ENROLL** (1-877-623-6765).

QUESTIONS?

*For more information about the Health Connector, please visit **MAhealthconnector.org** or call **1-877 MA-ENROLL** (1-877-623-6765) or TTY: 1-877-623-7773, Monday to Friday, 8:00 a.m. to 6:00 p.m.*

Does access to employer-based health coverage affect my eligibility for subsidized health insurance through the Health Connector?

An offer of health coverage from the Commonwealth of Massachusetts, as the employer, could affect your eligibility for these credits and subsidies through the Health Connector. If your income meets the eligibility criteria, you will qualify for credits and subsidies through the Health Connector if:

- **The Commonwealth of Massachusetts does not offer coverage to you, or**
- **The Commonwealth of Massachusetts offers you coverage, but:**
    - The coverage the Commonwealth of Massachusetts provides you (not including other family members) would require you to spend more than 9.5 percent of your household income for the year; or
    - The coverage the Commonwealth of Massachusetts provides does not meet the "minimum value" standard set by the new national health reform law (which says that the plan offered has to cover at least 60 percent of total allowed costs)

If you purchase a health plan through the Health Connector instead of accepting health coverage offered by the Commonwealth of Massachusetts please note that you will lose the employer contribution (if any) for your health insurance. Also, please note that the amount that you and your employer contribute to your employer-sponsored health insurance is often excluded from federal and state income taxes. Health Connector premiums have different tax treatment.

As part of considering whether the ACA and Marketplaces will affect you as an employee it is important to understand what the Commonwealth of Massachusetts offers you.

- The Commonwealth offers benefited employees health coverage through the Group Insurance Commission. To be eligible for GIC health insurance, a state employee must work a minimum of 18 ¾ hours in a 37.5 hour workweek or 20 hours in a 40 hour workweek. The employee must contribute to a participating GIC retirement system, such as the State Board of Retirement, a municipal retirement board, the Teachers Retirement Board, the Optional Retirement Pension System for Higher Education, a Housing, Redevelopment Retirement Plan, or another Massachusetts public sector retirement system (OBRA is not such a public retirement system for this purpose. Visit www.mass.gov/gic or see your GIC Coordinator for more information.
- Temporary employees, contractors, less-than-half time part time workers, and most seasonal employees are not eligible for GIC health insurance benefits. These employees may shop for health insurance through the Health Connector and may be eligible for advanced premium federal tax credits and/or state subsidies if their gross family income is at or below 400% Federal Poverty Level (which is approximately $46,000 for an individual and $94,000 for a family of four). Visit www.MAhealthconnector.org or call 1-877-MA-ENROLL for more information.

If there is any confusion around your employment status and what you are eligible for, please email healthmarketplacenotice@massmail.state.ma.us or contact your HR department or GIC Coordinator.

UMASS BOSTON
UNIVERSITY OF MASSACHUSETTS BOSTON
HUMAN RESOURCES

100 Morrissey Boulevard
Boston, MA 02125-3393
P: 617.287.5150
F: 617.287.5179
www.umb.edu/hr

POLICY & GUIDANCE MEMORANDUM

#2009-15: State Ethics Law (Revised May 1, 2018)

The Conflict of Interest Law seeks to prevent conflicts between private interests and public duties, foster integrity in public service, and promote the public's trust and confidence in that service by placing restrictions on what employees of the university may do on the job, hours after and after leaving public service.

This memorandum contains the annual notice of significant features of the State Ethics Law (M.G.L. c.268A). The conflict of interest law, M.G.L. c. 268A imposes "standards of conduct" on all state, county and municipal employees.

Incompatible Employment

First, § 23 (b)(1) prohibits public employees from accepting other employment involving compensation of substantial value, the responsibilities of which are inherently incompatible with the responsibilities of his public office.

Example: a police officer would be prohibited from serving as a private security guard in his town because his duties as a law enforcement official are incompatible with the demands of his private employer.

Unwarranted Privileges

Section 23(b)(2) prohibits a public employee from using or attempting to use his or her official position to secure for himself or others unwarranted privileges or exemptions which are of substantial value and which are not properly available to similarly situated individuals;

Example: A governmental official may not use his governmental time or resources, such as office space, word processors, telephones, photo copiers or fax machines, to conduct a private business. Section 23(b)(2) dictates that the use of public time and resources must be limited to serving public rather than private purposes.

The Commission has also emphasized that the use of one's public position to solicit or coerce special benefits, of substantial value, for oneself or others will constitute a use of one's official position to secure unwarranted privileges or exemptions not properly available to similarly situated individuals. In addition, the Commission has advised municipal officials that they must apply objective criteria to their official duties and that if, for example, a board member cannot be objective about a matter, he should abstain.

Appearance of Conflict

Section 23(b)(3) prohibits a public employee from acting in a manner which would cause a reasonable person, having knowledge of the relevant circumstances, to conclude that any person can improperly influence or unduly enjoy the public employee's favor in the performance of his or her official duties, or that he or she is likely to act or fail to act as a result of kinship, rank, position or undue influence of any party or person. It shall be unreasonable to so conclude if such officer or employee has disclosed in writing to his or her appointing authority or, if no appointing authority exists, discloses in a manner which is public in nature, the facts which would otherwise lead to such a conclusion.

Section 23(b)(3) has often been described as the section that covers "appearances" of conflicts of interest. The statute as it currently reads, however, does not use the term "appearance." It is worth emphasizing that §23(b)(3) prohibits acting "in a manner which would cause a reasonable person, having knowledge of the relevant circumstances, to conclude" that the official would be unduly influenced or unduly favor any party or person.

Example: A reasonable person could conclude that a board of health member might favor or disfavor his cousin's application. Although the cousin is not a member of his immediate family under §19, the family link would implicate §23(b)(3). To dispel such a reasonable conclusion, the board of health member should make a written disclosure to his appointing authority, describing the relevant facts of the family relationship and the official action, prior to his acting as a board member. If the board member were popularly elected, she must make a disclosure that is "public in nature." The Commission has advised that elected municipal officials should make such disclosures in writing and file them as public records with their municipal clerk. In some circumstances, it may also be prudent to reiterate the disclosure as part of the meeting minutes.

Confidential Information

Section 23(c)(1) prohibits a current or former municipal employee from accepting "employment or engag[ing] in any business or professional activity which will require him to disclose confidential information which he has gained by reason of his official position." Section 23(c)(2) prohibits him from "improperly disclos[ing] material or data within the exemptions to the definition of public records as defined by section seven of chapter four, and were acquired by him in the course of his official duties nor use such information to further his personal interest."

Adequate disclosure

Section 23(d) provides that "any activity specifically exempted from any of the prohibitions in any other section of this chapter shall also be exempt from the provision of this section. The state ethics commission . . . shall not enforce the provisions of this section with respect to any such exempted activity."

Example: Because adequate disclosure may be part of complying with §§19 or 20 (which were discussed in previous Ethics Primers), a municipal employee may comply with the disclosure requirements of §23(b)(3) by complying with the former. For further guidance regarding whether more than one disclosure is required, you should review the matter with municipal counsel or contact the Ethics Commission.

Training

Every 2 years, all state, county and municipal employees must complete a conflict of interest law online training program. Newly elected or appointed public employees must complete this training within 30 days of beginning public service, and every 2 years thereafter.

In addition, every year all state, county and municipal employees must be provided with the summary of the conflict of interest law. Newly elected or appointed public employees should be provided with the summary within 30 days of election or appointment, and on an annual basis thereafter. All public employees are required to sign a written acknowledgment that they have been provided with the summary.

For additional information, call the State Ethics Commission at (617) 371-9500 or visit their website at: www.mass.gov/orgs/state-ethics-commission

University of Massachusetts Boston
Department of Human Resources
100 Morrissey Blvd.
Boston, Massachusetts 02125
(617) 287-5150
www.umb.edu/hr

UMASS BOSTON
UNIVERSITY OF MASSACHUSETTS BOSTON
HUMAN RESOURCES

100 Morrissey Boulevard
Boston, MA 02125-3393
P: 617.287.5150
F: 617.287.5179
www.umb.edu/hr

POLICY & GUIDANCE MEMORANDUM

#2009-07: Political Activity (revised May 1, 2018)

Public employees -- employees and volunteers of state, county, and municipal agencies -- have most of the same rights as other citizens to engage in private political activity. However, the conflict of interest law, G.L. c. 268A, restricts some political activity of public employees. In addition, the campaign finance law, G.L. c. 55, restricts public employees' political fundraising. The campaign finance law is enforced by the Office of Campaign and Political Finance ("OCPF"). Questions regarding the campaign finance law should be directed to OCPF. This Advisory addresses restrictions on public employee political activity imposed by the conflict of interest law.

1. May Do: Political Activities by Public Employees That Generally Do Not Raise Conflict of Interest Law Issues

In general, public employees of all types may engage in private political activity, subject to the restrictions on political fundraising imposed by G.L. c. 55. The conflict of interest law does not prohibit a public employee from engaging in political activity on his own time, using his own or other private resources, and when he is acting for himself and not as an agent or representative of anyone else.

Below are further examples of election-related political activity that any public employee may do on his own time and without the use of his official title or public resources without raising any issue under the conflict of interest law:

- with his own stationery, computer, or wireless account, write letters to the editors or blog about political issues,
- distribute advocacy literature or hold a sign expressing his political views,
- with his own computer and email or wireless account, send emails or text messages expressing his political views,
- contribute his own funds in compliance with the campaign finance law to a campaign committee for a candidate or concerning a ballot question,
- answer voter survey questions, and
- vote in any election.

Similarly, public employees may engage in **non-election-related political activity on** their own time, without the use of public resources and as private citizens.

2. May Not Do: Political Activities by Public Employees That Generally Are Prohibited by the Conflict of Interest Law

In general, a public employee may not use his public position to engage in political activity. Section 23(b)(2)(ii) of the conflict of interest law prohibits the use of one's public position to engage in political activity, because a public employee who does so is using his official position to secure for himself or others (such as a candidate or a ballot question committee) unwarranted privileges of substantial value that are not properly available to similarly situated persons.

There are two exceptions to this general rule. First, elected officials, and public employees who hold policy-making positions, have more leeway to make statements about and take action concerning ballot questions, while using their public positions and public resources, than do appointed public employees who do not hold policy-making positions. Second, elected officials have greater latitude than non-elected public employees to engage in certain other election-related political activities. These exceptions are discussed in more detail below in sections 3 and 4.

Subject to these exceptions, a public employee **may not** engage in political activity, whether election-related or non-election related, on his public work time; while acting in his official capacity or while in his official uniform; in a public building (except where equal access for such political activity is allowed to all similarly situated persons); or with the use of other public resources, such as staff time, public office space and facilities, public office equipment such as computers, copiers, and communications equipment, public websites and links to public websites, or public office supplies such as official stationery.

A public employee who engages in such political activity, unless the activity is of truly minimal duration or significance (such as wearing a political campaign button to work in a public office), violates the conflict of interest law.

Below are further examples of election-related political activities that public employees MAY NOT DO. Public employees MAY NOT:

- send campaign-related emails using official computers or email,
- send campaign-related documents using official fax machines,
- use a public office telephone to make campaign-related calls,
- use on-duty public employees or public supplies, materials, or equipment to create, reproduce or distribute campaign materials,
- use official letterhead stationery, even if privately paid for, to advocate for or endorse a candidate or to support or oppose a ballot question,
- use any public seal, logo, or insignia, on campaign materials,
- use public office staff or equipment to do any of the following: conduct campaign research, write campaign or political speeches, conduct campaign polls, answer campaign questions, or create or maintain voter or supporter databases or campaign website or links,
- use public office staff or space for a press conference to endorse, promote or oppose a candidate or ballot question position,
- if appointed, use a public title while campaigning,
- if appointed, use a public title to endorse a candidate,
- if appointed, use a public title to support or oppose a ballot question (except to the extent appointed policy-makers are permitted to do so, as further discussed below in Section 3 of this Advisory),
- if appointed, perform election campaign tasks while on public work time,
- hold campaign planning meetings or any other campaign-related event in public office space, or

- wear a public employee uniform while performing campaign tasks or urging support for a particular candidate or measure.

Political fundraising is regulated by G.L. c. 55, the campaign finance law. In addition to the restrictions of Chapter 55, Section 23(b)(2)(ii) of the conflict of interest law prohibits all public employees - whether elected, appointed, or policy-making - from directly or indirectly soliciting political contributions of any kind, including personal services, in any situation where such a solicitation is inherently coercive.

A solicitation is inherently coercive, and therefore prohibited by the conflict of interest law, if it is directed by a public employee at his subordinate, persons or entities doing business with or having a matter pending before his public agency, or anyone subject to his or his agency's authority. By contrast, campaign contributions which are voluntarily made in response to a general rather than a targeted solicitation may be accepted from such sources if they are received and reported by the official's campaign committee in compliance with the campaign finance law.

The conflict of interest law also restricts the extent to which a public employee may represent campaigns and grass roots groups in dealings with government agencies. A public employee who is not serving in a "special" position may not represent a political campaign or a grass roots group in its dealings with public agencies at his level of government (state, county, or municipal), pursuant to Sections 4, 11 and 17 of the law.

These restrictions generally apply to "special" public employees only as to matters in which the employee participated, or for which the employee had official responsibility, or which is pending in the special public employee's agency.

If you are uncertain whether your position is a "special" position for purposes of the conflict of interest law, you should obtain advice from the Ethics Commission's Legal Division by calling (617) 371-9500, or online at www.mass.gov/ethics.

3. Non-Election-Related Political Activity: What Public Employees May and May Not Do

Not all political activity involves elections. Political activity may involve matters which will not be decided by election, or which will occur before any election has been scheduled. Examples of such political activity includes supporting or opposing town meeting warrant articles, municipal bylaw changes, and the other types of decisions set forth in the Introduction to this Advisory.

The prohibition of Section 23(b)(2)(ii) of the conflict of interest law against the use of official position to obtain or confer unwarranted privileges of substantial value applies to non-election-related political activity as well as to election-related activity. As with election-related activity, the applicable restrictions depend upon the particular public position that a person holds. This section of this Advisory describes the restrictions on non-election-related political activity under the conflict of interest law.

It is important to note that once an election is scheduled (or, in some cases, even just anticipated) concerning a matter, political activity relating to the matter will be deemed to be election-related political activity and a public employee's involvement in such activity will be subject to the greater restrictions described above in the sections of this Advisory concerning election-related political activity. Most importantly, election-related political activity is subject to the restrictions of the campaign finance

law and the public employee wishing to participate in such activity must observe those limits. Any action prohibited by the campaign finance law will generally be considered "unwarranted" for purposes of Section 23(b)(2)(ii). A public employee who is uncertain about the restrictions imposed by the campaign finance law should consult OCPF.

For a complete guide please visit https://www.mass.gov/advisory/11-1-public-employee-political-activity.

UMASS BOSTON
UNIVERSITY OF MASSACHUSETTS BOSTON
HUMAN RESOURCES

100 Morrissey Boulevard
Boston, MA 02125-3393
P: 617.287.5150
F: 617.287.5179
www.umb.edu/hr

Massachusetts Pregnant Workers Fairness Act

The Pregnant Workers Fairness Act, effective on April 1, 2018, expressly prohibits employment discrimination on the basis of pregnancy and pregnancy-related conditions, such as lactation or the need to express breast milk. It also describes employers' obligations to employees that are pregnant or lactating and the protections these employees are entitled to receive. Generally, employers may not treat employees or job applicants less favorably than other employees based on pregnancy or pregnancy related conditions. Employers also have an obligation to accommodate pregnant workers.

UMass Boston is committed to treating all employees and applicants fairly. We encourage all employee and applicants to discuss their needs and have any questions addressed so that the University remains inclusive and welcoming to all.

Under the Act:

- Upon request for an accommodation, the employer has an obligation to communicate with the employee in order to determine a reasonable accommodation for the pregnancy or pregnancy-related condition. This is called an "interactive process," and it must be done in good faith. A reasonable accommodation is a modification or adjustment that allows the employee or job applicant to perform the essential functions of the job while pregnant or experiencing a pregnancy-related condition, without undue hardship to the employer. "Undue hardship" means that providing the accommodation would cause the employer significant difficulty or expense.
- An employer must accommodate conditions related to pregnancy, including post-pregnancy conditions such as the need to express breast milk for a nursing child, unless doing so would pose an undue hardship on the employer.
- As with all reasonable accommodations, medical documentation generally is required. No documentation is needed, however, if the accommodation is requested for: (i) more frequent restroom, food or water breaks; (ii) seating; (iii) limits on lifting no more than 20 pounds; or (iv) private, non-bathroom space for expressing breast milk.
- An employer cannot require a pregnant employee to accept a particular accommodation, or to begin disability or parental leave if another reasonable accommodation would enable the employee to perform the essential functions of the job without undue hardship to the employer.

- An employer cannot refuse to hire a pregnant job applicant or applicant with a pregnancy-related condition, because of the pregnancy or the pregnancy-related condition, if an applicant is capable of performing the essential functions of the position with a reasonable accommodation.
- An employer cannot deny an employment opportunity or take adverse action against an employee because of the employee's request for or use of a reasonable accommodation for a pregnancy or pregnancy-related condition.

If you would like to request a reasonable accommodation, or have any questions or concerns about requesting accommodations, please contact ODEI at diversity@umb.edu. For a Request for Accommodation from, please visit: https://www.umb.edu/editor_uploads/images/odi/Request_for_Accommodation_Form... 11.9.pdf

- Employers must provide written notice to employees of the right to be free from discrimination due to pregnancy or a condition related to pregnancy, including the right to reasonable accommodations for conditions related to pregnancy.
- Employers must also provide written notice of employees' rights under the Act: (1) to new employees at or prior to the start of employment; and (2) to an employee who notifies the employer of a pregnancy or a pregnancy-related condition, no more than 10 days after such notification.

The Pregnant Workers Fairness Act is enforced by the Massachusetts Commission Against Discrimination (MCAD). Additional information regarding how to file a complaint that the Act has been violated and other related matters may be found on the MCAD website www.mass.gov/mcad.

The foregoing is a synopsis of the requirement under the Act, and both employees and employers are encouraged to read the full text of the law available on the General Court's website: https://malegislature.gov/Laws/SessionLaws/Acts/2017/Chapter54.

If you have questions about these new requirements, please contact Human Resources Benefits Unit at benefits@umb.edu or by calling 617-287-5150.

Doc. T16-040
Passed by the BoT
9/21/2016

UNIVERSITY OF MASSACHUSETTS
NON-DISCRIMINATION AND HARASSMENT POLICY

PURPOSE

The University of Massachusetts complies with applicable state and federal laws on non-discrimination, harassment, and retaliation including Title IX of the Education Amendments of 1972, Title VII of the Civil Rights Act of 1964, the Violence Against Women Act of 1994, and the Massachusetts anti-discrimination law. This policy states the University's commitment to assure compliance.

I. INTRODUCTION

This policy affirms the University of Massachusetts' ("University's") commitment to provide a welcoming and respectful work and educational environment, in which all individuals within the University community may benefit from each other's experiences and foster mutual respect and appreciation of divergent views. The University will not be tolerant of conduct which violates rights guaranteed by the law or University policies. Accordingly, the University prohibits unlawful discrimination and harassment based upon protected characteristics, and related retaliatory conduct, in accordance with state and federal non-discrimination laws, including Title IX of the Education Amendments of 1972, Title VII of the Civil Rights Act of 1964, the Violence Against Women Act of 1994, and the Massachusetts anti-discrimination laws.

II. POLICY STATEMENT

The University prohibits unlawful discrimination, harassment (including sexual harassment), and retaliation against anyone based on religion or religious belief, color, race, marital status, veteran or military status, age, sex, gender identity or expression, sexual orientation, national origin, ethnicity, disability, genetic information, or any other legally protected class, in education, admission, access to or treatment in, its programs, services, benefits, activities, and terms and conditions of employment at the University.

III. DEFINITIONS

For the purposes of this policy, the following definitions apply.

a. ***Unlawful discrimination*** is conduct that is directed at a specific person or persons that subjects them to treatment that adversely affects their employment, application

for employment, education, admissions, University benefits, programs, or activities, because of their religion or religious belief, color, race, marital status, veteran or military status, age, sex (including sexual harassment), gender identity or expression, sexual orientation, national origin, ethnicity, disability, genetic information, or any other legally protected class.

b. ***Harassment*** is conduct by a person or persons against another person or persons based upon their legally protected class that adversely has the effect of:

(i) unreasonably interfering with a person or person's employment, educational benefits, academic grades or opportunities, or participation in University programs or activities; or

(ii) unreasonably interfering with a person or person's work or academic performance; or

(iii) creating an intimidating, hostile, or offensive working or academic environment.

c. ***Sexual Harassment*** is unwelcome conduct of a sexual nature when:

(i) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment, education, or participation in University programs or activities; or

(ii) submission to or rejection of such conduct by a person or persons is used as a basis for employment or educational decisions affecting such person or persons, or participation in University programs or activities; or

(iii) such conduct unreasonably interferes with a person or person's work or academic performance; interferes with or limits a person or person's ability to participate in or benefit from a work or academic program or activity; or creates an intimidating, hostile, or offensive working or academic environment.

d. ***Retaliation*** is the interference through intimidation, including threats, coercion, or unlawful discrimination, with an individual's right or privilege secured under the law [Title IX of the Education Amendments of 1972, Title VII of the Civil Rights Act of 1964, the Violence Against Women Act of 1994, the Massachusetts anti-discrimination laws, or other laws] or interfering with an individual's right to make a complaint, testify, assist, or participate in any manner in an investigation, proceeding or hearing, or to intervene to prevent a violation of this policy.

Any member of the University community who engages in unlawful discrimination, harassment (including sexual harassment), or retaliation in violation of this policy may be subject to disciplinary or other action. The campuses shall develop campus policies and

complaint and investigatory procedures that will provide an equitable and prompt resolution of a complaint and make recommendations for disciplinary or other action.

This policy applies to all members of the University community, including students, employees, faculty, applicants for admissions and employment, contractors, volunteers, and visitors.

IV. RESPONSIBILITIES

Chancellors and the Senior Vice President for Administration & Finance and Treasurer for the President's Office are directed to disseminate this policy within their communities.

V. STANDARDS

The President or designee, in consultation with the General Counsel and Senior Vice President for Administration & Finance and Treasurer, will issue administrative standards to implement this policy. Campuses shall establish campus policies and procedures, within the scope of this policy and the administrative standards.

Doc. T92-037

Passed by the BoT

6/3/92

UNIVERSITY OF MASSACHUSETTS
SEXUAL HARASSMENT POLICY

Sexual harassment is sex discrimination and, therefore, a violation of federal and state law. It is the policy of the University of Massachusetts that no member of the University community may sexually harass another. For purposes of this policy and consistent with federal regulations, sexual harassment is defined as follows:

> Unwelcomed sexual advances, requests for sexual favors and other verbal or physical conduct of sexual nature constitute sexual harassment when: 1) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment or academic work, 2) submission to or rejection of such conduct by an individual is used as the basis for employment or academic decisions affecting such individual or 3) such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working or academic environment.

It is the policy of the University of Massachusetts to protect the rights of all persons within the University community by providing fair and impartial investigations of all complaints brought to the attention of appropriate officials. Any member of the University community found to have violated this sexual harassment policy will be subject to disciplinary action.

Chancellors are directed to take appropriate measures to inform each member of the University community of this policy statement and to develop procedures, in conjunction with the President's Office, for filing, hearing and resolving complaints.

Issuing Office: Human Resources **Policy Number**: FY15-HRS-006-00

Policy Name: Background Checks for New Benefitted Employees

Original Date Issued: February 4, 2015
Revision #: September 16, 2015
Last Update:

Purpose of Policy: The University of Massachusetts is committed to providing a safe and secure environment, supported by qualified employees that will allow all of its students, faculty, staff, and those associated with them to successfully carry out the University's teaching, research, and public service missions. As a condition of employment, the University will conduct appropriate background checks for all new hires. This policy will be implemented in a manner consistent with the rights of privacy, equal opportunity, and academic freedom afforded to those who serve the University, based on the University of Massachusetts Policy on Employee Background Reviews, Doc. T10-088, Passed by the BoT 12/8/10.

This policy standardizes the guidelines for reviewing the academic and personal backgrounds of new employees to foster integrity and a safe environment for the university community.

Applicable to:
This policy shall apply to all departments at UMass Boston, and specifically, the following employees:

- All employees who are appointed on a full-time or part-time benefitted basis.

This policy shall not apply to:

- Employees who are re-hired with a break in service less than one year will be deemed to have satisfied the requirements of this policy.

Note: Non-benefitted full-time and part-time employees, contingent workers, contractors, graduate and undergraduate student employees, and sensitive positions

Administration and Finance
100 Morrissey Blvd
Boston, Massachusetts 02125
(617)287-5100

will be included at a future date, as well as those promoted internally into another position.

Policy:
The review of the background check will be performed by:

- the vendor the University of Massachusetts has contracted with to perform background checks for UMass Boston,
- the assistant vice chancellor for human resources or designee who has been documented in writing, and
- the adjudication committee of 5 (five) members (one from each area); Human Resources, Office of Diversity and Inclusion, Chancellor's Office, Provost Office and the Department of Public Safety.

Only these individuals will have access to the information contained in the background checks. No printed/paper documents related to background checks will be available. All background check information is electronic.

A standard background check, at a minimum, shall consist of:

- the verification of education (highest degree obtained);
- the verification of previous employment (current employer, if any, and previous seven years,)
- the verification of licensure (where such licensure is required in the job description or is cited in a job posting, resume, curriculum vitae or cover letter);
- a criminal background check which includes both criminal and sex offender record information. A criminal background check includes a review of the candidate's criminal history record check under his/her current, maiden and any alias names, based on their social security # and the state(s) of residence during the last seven (7) years;
- the national sex offender search; and
- reference checks (performed by the department hiring manager).

The university may, depending on the nature of the position, conduct other background reviews, including reviews of credit records, motor vehicle records and other similar state or national searches.

Administration and Finance
100 Morrissey Blvd
Boston, Massachusetts 02125
(617)287-5100

Employees and candidates may receive a copy of their background check at no charge by requesting it from the university's vendor.

Procedures:

A statement related to employee background checks will be included in university employment information including job descriptions and postings.

University pre-employment forms and/or online application process will not include any requirement for the applicant to disclose any criminal convictions or pending criminal charges.

The successful candidate for each position must sign the offer letter accepting the position and authorizing a background check, as employment is conditional on the outcome of the check. A background check will not be processed without signed consent by the applicant. If the successful candidate does not sign the letter and return to Human Resources within two (2) weeks, the offer for employment will be immediately rescinded.

Background Check Internal Process:

The successful candidate may start employment prior to passing the background check; however, employment is contingent on passing the background check. Because of the sensitivity of the job, interaction with vulnerable populations, or any other reason, the hiring manager may decide not to have a candidate begin employment prior to the conclusion of the background check. Background checks usually take 5 (five) – 10 (ten) business days; however, it may take up to 30 (thirty) days depending on the state or office responding to the inquiry, or longer for international reviews.

Step 1: The successful candidate must authorize the university to perform a background check. A background check cannot be processed without the signed consent of the successful candidate. A successful candidate refusing to complete the acknowledgment section of his or her offer letter will not be considered for employment and the offer will be immediately rescinded.

Step 2: The background check process will commence when the signed offer letter is received by Human Resources (HR).

Administration and Finance
100 Morrissey Blvd
Boston, Massachusetts 02125
(617)287-5100

Step 3: HR submits the legal name and valid email address to the vendor who will email the successful candidate and begin the background check process.

Step 4A: If the candidate passes the background check, and has already started employment, no further action is needed. If the candidate has not started employment based on the sensitivity of the position, HR will notify the hiring manager via email.

Step 4B: If the background check includes any discrepancies in the areas of education, employment or licensure, the assistant vice chancellor for human resources or designee will review the discrepancies. If the AVC deems the candidate suitable for the position sought at the university, and the candidate has already started employment, no further action is needed. If the candidate has not started employment based on the sensitivity of the position, HR will notify the hiring manager via email. If the AVC determines the candidate unsuitable, s/he refers the report to the adjudication committee. Refer to step 4C.

Step 4C: If the background check includes any criminal history or sex offender history, the assistant vice chancellor for human resources or designee refers the report to the adjudication committee. The adjudication committee determinations will be based on criteria agreed to by the vice chancellors and will be reviewed periodically. The adjudication committee will make their decision within 3-5 business days.

- If the adjudication committee deems the candidate suitable, and the candidate has already started employment, no further action is needed. If the candidate has not started employment based on the sensitivity of the position, HR will notify the hiring manager via email.
- If the adjudication committee deems a candidate unsuitable for the position sought at the University, Human Resources will notify the vendor who will notify the candidate and the candidate has the opportunity to appeal. See below.

Step 5: The University reserves the right to immediately rescind an offer upon an unsuccessful background check.

Appeal Process

The appeal process is in accordance with the provisions of the Federal Fair Credit Reporting Act (FCRA) and Criminal Offender Record Information (CORI) law.

Administration and Finance
100 Morrissey Blvd
Boston, Massachusetts 02125
(617)287-5100

If adjudication committee deems a candidate unsuitable for the position sought at the University, HR will notify the vendor who will initiate the pre-adverse letter directly to the candidate.

The candidate will receive the entire background report and a summary of their rights to appeal. If the candidate believes that the reported background review information is inaccurate, s/he may appeal the accuracy of the background review information and to have such findings reviewed by the vendor conducting the background review. If the candidate does not appeal, the employment offer is closed and the vendor will mail an "adverse action letter," withdrawing the offer.

Recordkeeping:

Copies of conditional job offers for candidates who successfully complete a background check shall be filed in the candidate's personnel file. Copies of conditional job offer letters that do not result in employment shall be filed in a separate file. All background check information is held in the vendor system and is not printed and can only be reviewed by designated HR employees and members of the adjudication committee, as appropriate.

Other

This policy does not replace any federal or state statutory requirements to conduct certain background check reviews as a condition for employment for a specific occupation.

This policy will also follow and comply with all equal opportunity statutes, Federal Fair Credit Reporting Act (FCRA) and Criminal Offender Record Information (CORI) law.

Definitions

Vendor:

The vendor that the University of Massachusetts has contracted with to perform background checks for UMass Boston.

Adjudication Committee:

Administration and Finance
100 Morrissey Blvd
Boston, Massachusetts 02125
(617)287-5100

The adjudication committee of 5 (five) members (one from each area); Human Resources, Office of Diversity and Inclusion, Chancellor's Office, Provost Office and the Department of Public Safety that reviews unsuitable candidates before a final decision.

Oversight Department: Human Resources

Responsible Party within Department: Assistant Vice Chancellor for Human Resources

Monitoring:
There will be an annual review of this policy by HR, in consultation with the adjudication committee.

There will be a monthly review of all new employees of the prior month to insure that all have successfully passed their background checks and that all have been documented properly.

Authority:

Doc. T10-088, Passed by the BoT, 12/8/10 Policy on Employee Background Reviews.

Administration and Finance
100 Morrissey Blvd
Boston, Massachusetts 02125
(617)287-5100

Doc. T00-051
Passed by the BoT
8/2/00

UNIVERSITY OF MASSACHUSETTS
POLICY ON FRAUDULENT FINANCIAL ACTIVITES

POLICY STATEMENT AND PRINCIPLES

This policy is established to protect the assets and interests of the University, to increase overall fraud awareness, and to ensure a coordinated approach toward resolution of financial fraud.

The University must identify and promptly investigate all instances and allegations of fraudulent activities regarding University funds, documents, and equipment involving staff, faculty, students, vendors, agencies, or other parties. Good business practice dictates that suspected defalcation, misappropriation or other fiscal irregularities be promptly identified, and investigated. We believe that it is everyone's responsibility to report any possible fraudulent activity.

All persons found to have committed fraud relevant to University financial affairs shall be subject to punitive action by the University and investigation by law enforcement agencies when warranted.

Fraud in any form will not be tolerated. This policy applies to all University employees and will be enforced without regard to past performance, position held or length of service.

SCOPE AND DEFINITION OF FRAUD

Fraud generally involves a willful or deliberate act with the intention of obtaining an unauthorized benefit, such as money or property, by deception or other unethical means. All fraudulent acts are included under this policy and includes such things as:

- Embezzlement, misappropriation or other financial irregularities
- Forgery or alteration of documents (checks, time sheets, contractor agreements, purchase orders, other financial documents, electronic files)
- Improprieties in the handling or reporting of money or financial transactions
- Misappropriation of funds, securities, supplies, inventory, or any other asset (including furniture, fixtures or equipment)
- Authorizing or receiving payment for goods not received or services not performed
- Authorizing or receiving payments for hours not worked

The President shall issue guidelines to implement this Trustee policy and revise them as appropriate.

UNIVERSITY OF MASSACHUSETTS

FRAUDULENT FINANCIAL ACTIVITIES GUIDELINES
(Doc. T00-051)

These Guidelines are issued pursuant to the **Board of Trustees' Policy Statement on Fraudulent Financial Activities (Doc. T00-051, adopted August 2, 2000)**. Described herein are the steps to be taken when fraud, misappropriation, or similar dishonest activities are suspected.

Each campus will be responsible for developing procedures designed to comply with this University Guideline and informing all employees of the Policy on Fraudulent Financial Activities.

GENERAL PROTOCOL – REPORTING PROCEDURE

Anyone who believes fraud has occurred should report such incident. Employees are protected under Massachusetts General Law, Chapter 149, section 185, from retaliatory actions by the employer.

Use the channel of communication with which you are most comfortable. Accordingly, you may report your concerns to your immediate supervisor, department head, campus audit liaison, vice chancellor, chancellor, and/or directly to the University Auditor's Office or their campus police department.

Immediate supervisors, department heads, campus audit liaisons, vice chancellors, and chancellors must report all apparent cases of fraud brought to their attention to the University Auditor's Office, and if appropriate, to their campus police department. Please see the last section of this guideline for situations deemed Non-Fraud Irregularities, and reference the definition of fraud in Doc. T00-051.

RESPONSIBILITIES

University administrators and all levels of management are responsible for establishing and maintaining proper internal controls that provide security and accountability for the resources entrusted to them.

Administrators should be familiar with the risks and exposures inherent in their areas of responsibility and be alert for any indications of improper activities, misappropriation, or dishonest activity.

If the situation warrants immediate action – for example, obvious theft has taken place, security is at risk, or immediate recovery is possible – management and non-managerial staff receiving reports should immediately contact the responsible campus police department. In addition, follow the "General Protocol - Reporting Procedure."

Responsibilities of management and non-managerial staff for handling fraudulent activities include the following:

- Insure that notification promptly reaches the University Auditor's Office and the campus police department. Refer to the "General Protocol - Reporting Procedure."
- Do not contact the suspected individual to determine facts or demand restitution. Under no circumstances should there be any reference to "what you did", "the crime", "the fraud", "the forgery", "the misappropriation", etc.
- Managers should consult with campus or University human resources departments and University Counsel to determine if any immediate personnel actions are necessary.

- *Do not discuss the case, facts, suspicions, or allegations with anyone,* unless specifically directed to do so by the University Counsel, campus police, human resources, or the University Auditor's Office.
- Direct all inquires from any suspected individual, his or her representative, or his or her attorney to the University General Counsel. Direct all inquiries from the media to the campus news office.

The University Auditor's Office may investigate any suspected dishonest or fraudulent activity, which, in its opinion, may represent risk of significant loss of assets or reputation to the University. The University Auditor's Office may work with internal or external departments, such as the University General Counsel's Office, University and campus human resources departments, campus police departments, and Commonwealth law enforcement agencies, as circumstances may require.

Campus management will support the University's responsibilities and will cooperate with the University Auditor's Office and law enforcement agencies in the detection, reporting, and investigation of fraudulent acts, including prosecution of offenders. The University Auditor's Office has full, free and unrestricted access to all records and personnel of the University. Every effort should be made to effect recovery of University losses from responsible parties or through University insurance coverage.

Great care must be taken in dealing with suspected fraudulent activities to avoid any incorrect accusations, alerting suspected individuals that an investigation is under way, violating any person's right to due process, or making statements that could lead to claims of false accusation or other civil rights violation.

INVESTIGATION RESPONSIBILITIES

The University Auditor's Office will evaluate reported situations involving possible impropriety in financial matters pertaining to the University and make inquiries to the extent necessary to determine whether the allegation has substance. The campus audit liaison will be kept apprised of these activities. *The University Auditor's Office is available and receptive to receiving relevant information on a confidential basis and may be contacted directly whenever a fraudulent activity is suspected.*

When warranted, an internal investigation will be conducted. The Auditor's Office will proceed as follows if evidence is uncovered showing possible dishonest or fraudulent activities.

- Notify the campus audit liaison, respective area management and University General Counsel.
- Advise management to meet with the campus human resources director to determine if any immediate disciplinary personnel actions should be taken.
- Coordinate the notification of insurers and filing of claims with the Treasurer's Office Risk Manager. The Treasurer is responsible for notifying the bonding companies and filing bonding claims.
- Advise the campus on requirements to notify the Office of the State Auditor as required by Chapter 647 of the Acts of 1989.
- If federal funds are involved, determine the required federal reporting in cooperation with University General Counsel.

- If illegal activity is indicated, the responsible campus police department will be notified to coordinate the investigation. If illegal activity appears to have occurred, the findings will be reported to the appropriate agency for review, such as the District Attorney and/or Attorney General. This will be coordinated with University General Counsel.

- The University Auditor's Office will review the results of any investigations with responsible management and cognizant administrators as necessary, making recommendations for improvement to the systems of internal control.

NON-FRAUD IRREGULARITIES

Identification or allegations of acts outside the scope of this policy, such as personal improprieties or irregularities, whether moral, ethical, or behavioral, safety or work environment related, or complaints of discrimination or sexual harassment, should be resolved by the respective area management in conjunction with human resources and/or reference to any other existing University guidance or resource. Examples include the scholarly and research misconduct policy, the principles of employee conduct, the policy against intolerance, the sexual harassment policy, and the MGL Chapter 268A conflict of interest law (this list is not all-inclusive). The campus Ombuds Office or Equal Opportunity Office may also be of assistance.

The University Auditor's Office or University General Counsel may be contacted if guidance is needed to determine if an action might constitute fraud as defined in this policy.

DOC. T96-136, as amended
Passed by the BoT
12/4/96

UNIVERSITY OF MASSACHUSETTS
PRINCIPLES OF EMPLOYEE CONDUCT

Institutions of higher education are entrusted with great resources and commensurably great responsibilities. They must meet their mission of research, teaching, and service in ways that truly enrich the society that supports them and truly serve the students, parents, and alumni who in joining the university community become life-long members of the extended university learning family. College and university leaders play a key role in assuring that high standards of ethical practice attend to the delivery of services to their various constituents and to the custody and use by all their faculty, staff and students of the resources entrusted to them. The University of Massachusetts embraces the values expressed in these Principles of Employee Conduct and expects their observance by all its employees.

University employees are entrusted with public resources and are expected to understand their responsibilities with respect to conflicts of interest and to behave in ways consistent both with law and with University policy.

University employees are expected to be competent and to strive to advance competence both in themselves and in others.

The conduct of University employees is expected to be characterized by integrity and dignity, and they should expect and encourage such conduct by others.

University employees are expected to be honest and conduct themselves in ways that accord respect to themselves and others.

University employees are expected to accept full responsibility for their actions and to strive to serve others and accord fair and just treatment to all.

University employees are expected to conduct themselves in ways that foster forthright expression of opinion and tolerance for the view of others.

University employees are expected to be aware of and understand those institutional objectives and policies relevant to their job responsibilities, be capable of appropriately interpreting them within and beyond the institution, and contribute constructively to their ongoing evaluation and reformulation.

The University is responsible for communicating to University employees the content of these Principles of Employee Conduct and for ensuring that the standards of conduct contained herein are met.

The University expects to provide its employees:

a work environment that is professional and supportive;

a clear sense of the duties of their job, the procedures for performance review, and access to relevant University policies and procedures;

within the scope of each employee's assigned areas of authority and responsibility, the duty to exercise appropriate judgment and initiative in performing duties;

the right to seek appropriate review of matters that violate the ethical principles contained in these Principles.