Table of Contents

Introduction ........................................................................... 1
Internal Controls: An Overview ........................................... 3
Control Environment ......................................................... 6
Risk Assessment ............................................................... 7
Programmatic Controls ...................................................... 9
Administrative and Fiscal Controls ...................................... 11
Information and Communications ...................................... 13
Monitoring ................................................................. 21
Works Cited ....................................................................... 22
Appendix 1 ....................................................................... 23
Appendix 2 ....................................................................... 26
Appendix 3 ....................................................................... 28
Appendix 4 ....................................................................... 31
Department Wide Risk Assessment ................................. 32

Policies and Procedures
  Budget ........................................................................... 37
  Cash Receipts ............................................................... 47
  Grants and Contracts .................................................... 56
  Payroll ......................................................................... 75
  Purchases and Accounts Payable .................................... 87
  Revenue and Accounts Receivable ................................. 101

Data and Computing Guidelines ....................................... 109
  Definitions ................................................................... 121
  Data Security and Classification Guidelines .................. 141

University E-mail communications policy ....................... 148

Computing Services Guidelines Summary ....................... 149

Policy on Fraudulent Activities ....................................... 152
  Principles of Employee Conduct ................................. 153
  University Fraudulent Activities Guidelines ................ 155
Introduction

Massachusetts General Laws Chapter 647 of the Acts of 1989, An Act Relative To Improving The Internal Controls Within State Agencies, was passed into law on January 3, 1990 and became effective April 3, 1990 (Appendix 1). The law establishes internal control standards that define the minimum level of quality acceptable for internal control systems in operation throughout the various state agencies and departments. Those standards are outlined below.

- **Documentation** - Internal control systems of the agency are to be clearly documented and readily available for examination.

- **Transactions** - All transactions and other significant events are to be promptly recorded, clearly documented and properly classified.

- **Authority** - Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority.

- **Segregate Duties** – Essential duties and responsibilities should be assigned systematically to ensure that effective checks and balances exist. They include:
  1. Authorizing, approving, and recording transactions,
  2. Issuing and receiving assets,
  3. Making payments, and
  4. Reviewing or auditing transactions

- **Supervision** - Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved.

- **Access** - Access to resources and records is to be limited to authorized individuals as determined by the department head. The department head is responsible for maintaining accountability for the custody and use of resources and shall assign qualified individuals for that purpose. Periodic comparison shall be made between the resources and the accounting records to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts.

Chapter 647 requires that a *senior official*, equivalent in title to an assistant or deputy to the department head, in addition to his or her regular duties, be assigned the responsibility for the department’s internal control. This individual is the department’s Internal Control Officer. The Internal Control Officer’s organizational responsibilities include the following:
University of Massachusetts  
Dartmouth Campus  
Internal Control Plan

Introduction

- Have available on file written documentation of the department’s internal accounting and administrative control system for review by the Comptroller's Office, the Office of the Secretary of Administration and Finance, and the Office of the State Auditor,

- Evaluate the effectiveness of the agency’s internal control system at least annually, more often if conditions warrant. At that time, establish and implement any changes necessary to ensure the continued integrity of the system,

- Evaluate the results of audits and recommendations to improve departmental internal controls promptly,

- Implement timely and appropriate corrective actions in response to an audit and

- Address all actions determined as necessary to correct or otherwise resolve internal control matters in the department's budgetary request to the Governor and Legislature.

- Immediately report all variances, losses, shortages, or thefts of funds or property to the Office of the State Auditor. The statute specifically requires this action.

The State Auditor’s Office (SAO) reviews reported variances, losses, shortages, or thefts to determine the amount involved and report the facts surrounding the condition to the appropriate management and law enforcement officials. SAO then determines the internal control weaknesses that allowed the problem to occur, recommending changes to department management to correct these weaknesses. Department management must immediately implement policies and procedures necessary to prevent a reoccurrence of the condition, based on the SAO recommendations. (See Appendix 2 for reporting form.)

The Office of the State Auditor participates in establishing guidelines for reviewing departmental internal control plans. As part of their work on the Statewide Single Audit, SAO also reviews department plans.
The American Institute of Certified Public Accountants defines internal control as a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

(a) effectiveness and efficiency of operations,

(b) reliability of financial reporting, and

(c) compliance with applicable laws and regulations.

Every organization, be it governmental, for profit, or not-for-profit, exists to achieve some purpose or goal. The University's goals are outlined in its mission statement (Appendix 3). It is the role of management to provide the leadership needed for the University to achieve its goals and objectives. Internal controls are a coordinated set of policies and procedures for achieving management objectives.

A comprehensive framework of internal controls consists of the following five interrelated components.

(a) **Control Environment.** This is the foundation for all other components of internal control encompassing such factors as integrity and ethical values, commitment to competence, board of trustees and audit committee participation, management’s philosophy and operating style, organizational structure, assignment of authority and responsibility, and human resource policies and practices.

(b) **Risk Assessment.** This component identifies, analyzes, and manages the potential risks that could prevent management from achieving its objectives. Change is one factor that can be used to identify risks. Another is inherent risk usually associated with assets that can be readily converted to personal use.

(c) **Control Activities.** These are the policies and procedures needed to address the risks identified that could prevent management from achieving its objectives. Control activities generally relate to proper authorization of transactions, security of assets and records, and segregation of incompatible duties.

(d) **Information and Communication.** Information provided to staff should be appropriate in content, timely, current, accurate, and accessible. Communication takes such forms as policy manuals, accounting and financial reporting manuals, policy memoranda, and regularly scheduled staff meetings.
Internal Control Plan

Internal Controls: An Overview

(e) Monitoring. It is the responsibility of management to continually monitor control activities to ensure that they function properly and take the necessary corrective action to resolve potential problems or weaknesses in a timely manner. This component also involves evaluating the effectiveness of controls, i.e., (1) controls are properly designed so they will accomplish their intended purpose and (2) controls actually function as designed.

Programmatic Controls

As an institution of higher learning, the University of Massachusetts is a member of the New England Association of Schools and Universities, a non-profit, self-governing organization and one of six regional accrediting bodies in the United States, having as its primary purpose the accreditation of educational institutions. Through its evaluation activities, the Association provides public assurance about the quality of education of those schools and universities that wish to maintain membership.

Institutions of higher learning achieve accreditation from the New England Association through its Commission on Institutions of Higher Education by demonstrating they meet the Commission's Standards for Accreditation and comply with its policies. The Standards for Accreditation establish minimum criteria for institutional quality.

In addition, the Commission adopts policies which elucidate the Standards and relate to their application. Moreover, the Commission expects affiliated institutions to work toward improving their quality, increasing their effectiveness, and continually striving toward excellence. Its evaluative processes are designed to encourage such improvement.

Each of the eleven Standards encompasses a principal area of institutional activity. In applying the Standards, the Commission assesses and makes a determination about the effectiveness of the institution as a whole. The institution which meets the Standards:

- Has clearly defined purposes appropriate to an institution of higher learning;
- Has assembled and organized those resources necessary to achieve its purposes;
- Is achieving its purposes;
- Has the ability to continue to achieve its purposes.

Institutions of higher learning desiring recognition by the New England Association are expected to abide by the Standards. Affiliated universities and universities manifest their integrity through continued voluntary adherence to these criteria. Compliance is periodically reviewed through peer evaluations. These are preceded by self-studies directed toward demonstrating both adherence to the Standards and institutional improvement. The self-regulatory nature of accreditation assumes that institutions agree to participate in and to accept and profit by an honest and forthright assessment of institutional strengths and weaknesses.
Administrative and Fiscal Controls

The design and evaluation of controls over accounting and financial reporting is made more manageable by grouping similar or related activities into what are commonly referred to as “control cycles.” This approach also provides a logical framework and underscores the relationships that exist among the many control-related policies and procedures.

Control cycles are generally defined by business processes within the organization having to do with sources and uses of funds. Each control cycle has specific objectives and potential risks that can prevent management from meeting its objectives. A practical means of identifying potential risks or weaknesses is by using management’s implicit assertions of (1) existence or occurrence, (2) completeness, (3) rights and obligations, (4) allocation, (5) presentation and disclosure.

Control-related policies and procedures designed to compensate for such risks are categorized as follows: (1) authorization, (2) properly designed records, (3) security of assets and records, (4) segregation of incompatible duties, (5) periodic reconciliations, (6) periodic verifications, (7) analytical review, (8) and timely preparation of financial reports in conformity with generally accepted accounting principles.

The following control cycles have been identified as significant to the University in achieving its goals and objectives: (1) budgetary process, (2) revenue cycle - revenue, accounts receivable, and cash receipts, (3) purchasing cycle - expenditures, payables, and cash disbursements, (4) payroll cycle, (5) and resource management – cash, investments, and fixed assets.
University of Massachusetts
Dartmouth Campus
Internal Control Plan

Control Environment

Overall Objective
The organization shall provide for discipline and structure and promote integrity and ethical values to staff at all levels for the purpose of attaining its objectives and meeting its responsibilities.

Specific Objectives
1. The organization has a statement of mission and objectives.
2. There is a current organizational chart in use which fixes authority and responsibility and appropriate lines of reporting.
3. The organization has established an official code of conduct or an official set of policies governing employee conduct.
4. The organization has established and maintains up-to-date job descriptions for all employees.
5. The organization follows appropriate hiring policies.
6. Authority and responsibility are assigned in an appropriate manner.
7. Employees are properly trained.
8. Employees are periodically reviewed and performance is documented.
9. The organization has established performance goals and criteria for promotion.
10. The organization has developed and maintains a formalized policies and procedures manual.
11. The organization has established a budgetary control system.
12. The governing board has established an audit committee.
13. The organization has established an internal audit function.
The definition of internal control includes all aspects of an organization’s activities. In preparing a department-wide internal control plan, the starting point is the identification and analysis of risks that could prevent the organization from reaching its goals and objectives as defined by its mission statement. The following risk assessment was conducted by senior management.

1. **Financial fraud committed against the University** – assets converted to personal use depriving the organization of resources needed to achieve its goals and objectives.

2. **Loss of federal/state student financial aid eligibility** – seriously impact the level of resources available to the student population and student access to programs and services.

3. **Qualified opinion from independent financial auditors** – inability to enter into or maintain debt covenants and other contractual agreements.

4. **Failure to maintain compliance with federal and state funding agencies** – restitution of funds, loss of contracts and reduction in programs and services.

5. **Loss of accreditation** – reduction in programs and services including loss of federal funds preventing the University from achieving its goals and objectives.

6. **Lack of student demand and success** – indicative of program weaknesses and the ability of the University to maintain a competitive position with respect to its peers.

7. **Poor academic reputation and competitive position** – inability to attract quality students and faculty further impacting programs and services and the ability of the University to achieve its goals and objectives.

8. **Poor financial health and performance** – inability to provide the resources necessary to maintain a high quality and competitive academic program necessary for the University to achieve its goals and objectives.

9. **Poor condition of facilities** – failure to comply with health, safety, environmental and other regulations and mandates resulting in the closing of buildings and negatively impacting the learning environment.

10. **Failure to attract and retain quality faculty and staff** – inability to offer programs and services critical to the mission of the University.

11. **Early Retirement Incentive Program (ERIP)** – must service the student population and meet its business needs with a substantially reduced workforce, putting additional pressures on the remaining workforce, and jeopardizing the University’s ability to meet its goals and objectives.
12. Information technology security and access – unauthorized access from both internal and external sources could compromise the integrity of the information database and severely impact the ability of the University to service its student population and meet its business needs.

13. Lack of disaster recovery planning – inability to provide high system availability and recoverability in the event of hardware/infrastructure failure severely impacting the University’s ability to service its student population and meet its business needs.

14. Lack of business resumption planning – inability to provide services for an extended period of time due to a major catastrophic event.

15. NCAA violations and accreditation – limiting the opportunities for student athletes to participate in a broad range of varsity level sports.
University of Massachusetts
Dartmouth Campus
Internal Control Plan

Programmatic Controls

Mission and Purposes
The institution has a mission and a set of purposes appropriate to higher education, consistent with its charter or other operating authority, and implemented in a manner that complies with the Standards of the Commission on Institutions of Higher Education.

Planning and Evaluation
The institution undertakes planning and evaluation appropriate to its needs to accomplish and improve the achievement of its mission and purposes.

Organization and Governance
The institution has a system of governance that facilitates the successful accomplishment of its mission and purposes. Through its organizational design and governance structure, the institution creates and sustains an environment that encourages teaching, learning, scholarship, and where appropriate research, and it assures provision of support adequate for the appropriate functioning of each organizational component.

Programs and Instruction
The institution’s programs are consistent with and serve to fulfill its mission and purposes. Each educational program demonstrates consistency through its goals, structure, and content; policies and procedures for admission and retention; instructional methods and procedures; and the nature, quality, and extent of student learning and achievement. The institution provides sufficient resources to sustain and improve programs and instruction.

Faculty
Faculty qualifications, numbers, and performance are sufficient to accomplish the institution’s mission and purposes. Faculty competently offer the institution’s academic programs and fulfill those tasks appropriately assigned them.

Student Services
The institution provides an environment which fosters the intellectual and personal development of its students consistent with its mission and purposes and mode of educational delivery. It is sensitive to the non-academic needs of its students and recognizes that their educational experience consists of an academic component and interrelated developmental opportunities provided through a co-curricular program of student services. These services are guided by a philosophy, disseminated and reviewed on a regular basis, which is conducive to the development of a shared learning community and which prepares students to become responsible members of society.
Programmatic Controls

Library and Information Resources
The institution makes available the library and information resources necessary for the fulfillment of its mission and purposes. These resources support the academic and research program and the intellectual and cultural development of students, faculty, and staff. Library and information resources may include the holdings and necessary services and equipment of libraries, media centers, computer centers, language laboratories, museums, and any other repositories of information or technological systems required for the support of institutional offerings. Clear and disseminated policies govern access, usage, and maintenance of the library, information resources, and services. The institution ensures that students use these resources as an integral part of their education.

Physical Resources
The institution has sufficient and appropriate physical resources, including laboratories, network infrastructure, materials, equipment, and buildings and grounds, whether owned or rented; these are designed, maintained, and managed at both on- and off-campus sites to serve institutional needs as defined by its mission and purposes. Classrooms and laboratories, real or virtual, and other facilities are appropriately equipped and adequate in capacity. Proper management, maintenance, and operation of all physical facilities and virtual environments, are accomplished by adequate and competent staffing.

Financial Resources
The institution is financially stable. Ostensible financial stability is not achieved at the expense of educational quality. The institution’s financial resources are sufficient to sustain the achievement of its educational objectives and to further institutional improvement now and in the foreseeable future. The institution reallocates resources as necessary to achieve its purposes and objectives. All or substantially all of the institution’s revenue is devoted to the support of its educational purposes and programs. The institution has the ability to respond to financial emergencies and unforeseen circumstances.

Public Disclosure
In presenting itself to students and other members of the interested public, the institution provides information that is complete, accurate, and clear.

Integrity
The institution subscribes to, exemplifies, and advocates high ethical standards in the management of its affairs and in all of its dealings with students, faculty, staff, external agencies and organizations, and the general public.
Administrative and Fiscal Controls

Budgetary Process
The authorized budget should reflect anticipated revenues and appropriations.

Specific Objectives

(a) Budget Preparation

1. Responsibilities for budget preparation, adoption, execution, and reporting are segregated.
2. Budgets are prepared for all significant activities.
3. The budgeting system is integrated with the planning process.
4. The budget is prepared in sufficient detail to provide a meaningful tool with which to monitor subsequent performance.
5. The type of budgeting performed is compatible with the accounting system.
6. Interfund and interdepartmental transfers are included in the budget.
7. Procedures have been adopted and communicated to establish authority and responsibility for transfers between budget categories.

(b) Budget Approval

1. Original budget and budgetary amendments (including supplemental appropriations and budget transfers) are submitted to the governing body for approval.
2. A budget calendar is used for the orderly submission and approval of the budget.

(c) Budget Accounting and Reporting

1. Estimated revenues and appropriations are recorded in the accounting records for later comparison to actual amounts realized or incurred.
2. Actual expenditures are compared to the budget on a timely basis with reasonable (monthly) frequency.
3. Reports are discussed with departmental personnel and significant variations from budget are documented.
4. Management and the governing body are notified of expenditures in excess of budget.
Revenue Cycle
Revenue controls should be designed to ensure that University funds are collected, deposited, and accurately reported.

Specific Objectives
(a) Revenue and Accounts Receivable

1. Tuition and fees are authorized and periodically reviewed by the governing board.
2. An accounts receivable event is established whenever goods or services have been provided and corresponding earnings are measurable.
3. The responsibility of billing revenues is segregated from collections and general ledger posting.
4. Procedures exist for the timely billing of amounts due.
5. Balances of individual receivable accounts are periodically reconciled with general ledger control accounts.
6. Delinquent accounts are reviewed and considered for charge-off on a timely basis.
7. Write-offs and other reductions of receivables and refunds of amounts previously collected follow prescribed policies and procedures.
8. Tuition and fee waivers, bad debt write-offs, credit memos and allowances are approved independently of processing, recording, and collecting the charge.
9. Accounts receivables are established when expenditure reimbursement claims are submitted to Federal and State granting agencies and private contracts.

(b) Cash Receipts

1. Receipts are accounted for and balanced to reported collections on a daily basis.
2. Receipts are deposited intact on a daily basis.
3. Facilities exist for protecting undeposited cash receipts.
4. The responsibility for collecting, controlling, and depositing funds is segregated from maintaining accounting records.
5. Responsibilities for cash receipts are segregated from those for cash disbursements.
6. Timely bank reconciliations are prepared and reviewed by someone independent of the cash receipts function.
Purchasing Cycle

Acquisition of goods and services is properly controlled, accounted for, and in compliance with the institution’s purchasing regulations.

Specific Objectives

(a) Purchases and Accounts Payable

1. Purchases of goods and services are initiated by properly authorized requisitions bearing the approval of officials designated to authorize requisitions.

2. Unobligated funds are verified by the accounting or budget department as sufficient to meet the proposed expenditure.

3. Encumbrance entries are recorded only on the basis of approved purchase orders.

4. Competitive bidding procedures are used.

5. Purchase orders and contracts are issued under numerical or other suitable control.

6. Changes to purchase orders and contracts are subjected to the same controls and approvals as the original agreement.

7. An adequate record of open purchase orders and purchase agreements is maintained to ensure knowledge of outstanding commitments.

8. Procedures exist to verify that goods and services have been received, prices are as ordered, and the goods and services meet quality standards.

9. Procedures exist to record and follow up on partial deliveries.

10. The accounting and purchasing department are promptly notified of returned purchases, and such purchases are correlated with vendor credit advices.

11. Controls exist for submission and approval of reimbursements to employees for travel and other expenses.

12. Controls exist for processing invoices not involving materials or supplies, e.g., lease or rental payments and utility bills.
Administrative and Fiscal Controls

Specific Objectives

(a) Purchases and Accounts Payable

13. Balances of individual payable accounts are periodically reconciled with general ledger control accounts.

14. Access to the master vendor file is limited to employees authorized to make changes.

15. Responsibilities for the requisitioning and receiving functions are segregated from the purchasing, invoice processing, accounts payable, and general ledger functions.

(b) Cash Disbursements

1. Procedures exist for disbursement approval and warrant or check signing.

2. Responsibilities for the disbursement approval function are segregated from those for the disbursement, voucher preparation, and purchasing functions.

3. Controls are maintained over the supply of unused and voided warrants or checks.

4. The drawing of warrants or checks to cash or bearer is prohibited.

5. Controls exist over warrant or check signing machines as to signature plates and usage.

(c) Grants and Contracts

1. Grant disbursements are processed under the same degree of controls applicable to the organization’s other transactions, i.e., budget, procurement, etc.

2. Procedures are modified when funds are disbursed under grant or loan agreements and related regulations impose requirements that differ from the entity’s normal policies.

3. Procedures and controls exist to provide reasonable assurance that only eligible individuals receive assistance under Federal award programs and that amounts provided to or on behalf of eligibles were calculated in accordance with program requirements.

4. Procedures and controls exist to provide reasonable assurance that the draw down of Federal cash is only for immediate needs.

5. Controls exist to provide reasonable assurance that Federal funds are used only during the authorized period of availability.

6. Controls exist to ensure that costs charged to grants are in compliance with grant agreements.
Administrative and Fiscal Controls

Specific Objectives

(c) Grants and Contracts

7. Procedures exist for obtaining grantor approval before incurring expenditures in excess of budgeted amounts or for unbudgeted expenditures.

8. Procedures exist to identify, before order entry, costs and expenditures that are not allowable under grant programs.

9. If an indirect cost allocation plan is established, it has been developed in accordance with grantor requirements and approved as required by the grantor.

10. Grant activity is accounted for so that it can be separated from the accounting for locally funded activities.

11. Procedures exist to monitor compliance with grant requirements.

12. The level of authority for approving grants and contracts appears appropriate.
Payroll Cycle
All payrolls should be supported by appropriate evidence for authorized work actually performed and properly reflected in the accounting records.

Specific Objectives

(a) Initiating Payroll Transactions

1. Wages and salaries are approved by the governing board as part of the budget process.
2. Bonuses and employee benefits are authorized by the governing board.
3. All changes in employment (additions and terminations), salary and wage rates, and payroll deductions are properly authorized, approved, and documented.
4. Notices of additions, separations, and changes in salaries, wages, and deductions are promptly reported to the payroll-processing function.
5. Changes to the master payroll file are approved and documented.
6. Access to the master payroll file is limited to employees who are authorized to make changes.
7. Responsibilities for supervision and timekeeping functions are segregated from personnel, payroll processing, disbursement, and general ledger functions.
8. Records and controls exist for timekeeping and attendance.
9. Hours worked, overtime hours, and other special benefits are reviewed and approved by the employee’s supervisor.
10. Appropriate payroll records are maintained for accumulated employee benefits, i.e., sick leave, vacation, pension.
11. Procedures exist for authorizing, approving, and recording vacations, holidays, sick leave, and compensatory time.

(b) Processing Payroll

1. Payroll is calculated using authorized pay rates, payroll deductions, and time records.
2. Account coding procedures exist to ensure proper classification of employee compensation and benefit costs in general ledger accounts.
3. Responsibilities for the payroll processing function are segregated from personnel and general ledger functions.
Administrative and Fiscal Controls

Specific Objectives

(b) Processing Payroll

4. Controls exist to ensure that employee benefit and compensation costs do not exceed appropriated or budgeted amounts.

5. Accrued liabilities for unpaid employee compensation and benefit costs are properly recorded and disclosed.

6. Signature plates and the use of the payroll check-signing machine are kept under control of the official whose name appears on the signature plate (or his/her designee).

7. The supply of unused payroll checks is controlled.

8. A separate, imprest-basis, payroll account is maintained.

9. The payroll bank account is reconciled regularly by employees independent of all other payroll transaction processing activities.

10. Responsibilities for payroll distribution are segregated from personnel, timekeeping, and payroll processing functions.
Resource Management – Cash, Investments, and Fixed Assets

Cash, investments, and fixed assets should be supported by appropriate evidence for authorization, physically safeguarded, and properly reflected in the accounting records.

Specific Objectives

(a) Cash

1. Bank accounts are properly authorized.
2. Procedures exist to review bank balances for appropriate insurance and collateral on a periodic basis.
3. Procedures exist for steps essential to an effective bank statement reconciliation.
4. Responsibilities for preparing and approving bank account reconciliations are segregated from those for other cash receipt or disbursement functions.
5. Cancelled checks are subject to appropriate escheat procedures.
6. Controls and physical safeguards exist for petty cash funds.

(b) Investments

1. Investment policies are formally established and periodically reviewed.
2. Authority and responsibility has been established for investment opportunity evaluation and purchase.
3. Procedures have been established governing the level and nature of approvals required to purchase or sell investments.
4. Responsibilities for initiating, evaluating, and approving investment transactions are segregated from those for detail accounting, general ledger, and other related functions.
5. Adequate physical safeguards and custodial procedures exist over (a) negotiable and nonnegotiable securities owned and (b) legal documents or agreements evidencing ownership or other rights.
6. All securities are registered or held in the name of the entity.
7. Securities are periodically inspected or confirmed with safekeeping agents.
8. Detailed accounting records are maintained for investments.
9. Procedures exist to ensure that transactions arising from investments are properly processed, including income and amortization entries.
Specific Objectives

(b) Investments

10. Detailed accounting records for investments are periodically agreed to the general ledger.

11. Appropriate procedures exist to determine the fair value of investments.

12. The entity has an established policy for reporting investments as cash and cash equivalents.

(c) Fixed Assets

1. Written executive or legislative approval is required for all significant fixed asset projects or acquisitions.

2. Responsibilities for initiating, evaluating, and approving capital expenditures, leases, and maintenance or repair projects are segregated from those for project accounting, property records, and general ledger functions.

3. Those individuals authorized to initiate fixed asset transactions are identified and there is clear definition of the limits of their authority.

4. Controls exist to (a) distinguish between capital and operating budget expenditures, (b) identify operating budget expenditures to be capitalized as fixed assets, and (c) distinguish between capital and operating leases.

5. Controls exist ensuring that purchased materials and services for capital expenditure and repair projects are subject to the same levels of controls as exist for all other procurements.

6. Controls exist providing for obtaining grantor approval, if required, for the use of grant funds for fixed asset acquisitions.

7. Grant-funded authorizations are subject to the same controls as internally funded acquisitions.

8. The general ledger and detailed fixed asset records are updated for fixed asset transactions on a timely basis.

9. Physical safeguards over assets exist.

10. Periodic inventories of fixed assets are taken and inventory results are compared to detailed property records and general ledger control accounts.

11. Controls exist to govern depreciation methods and practices.

12. Controls exist for authorizing, approving, and documenting sales or other dispositions of fixed assets.
Information and Communication

Overall Objective

Information is current, accurate, appropriate in content and made available on a timely basis at all staff levels to permit management to achieve its objectives.

Specific Objectives

1. Accounts are maintained to ensure observance and limitations placed on the use of available resources.

2. Adequate source documentation exists to support amounts and items reported.

3. Assigned authorization levels and approvals exist for posting transactions to the general ledger.

4. A recordkeeping system is established to ensure that accounting records and documentation are retained for the time period required in accordance with the provisions of laws, regulations, contracts and grant agreements.

5. Procedures exist to ensure that reports are provided timely to managers for review and appropriate action.

6. Procedures exist for review and reconciliation of control accounts in the general ledger to subsidiary ledgers.

7. Computer and program controls exist and include:
   a. Data entry controls, i.e., edit checks.
   b. Exception reporting.
   c. Access controls.
   d. Reviews of input and output data.
   e. Computer general controls and security controls.

8. Operating policies and procedures are clearly written and communicated.

9. Staff meetings are regularly scheduled.

10. The governing Board conducts regular meetings where financial information is reviewed and the results of program activities and accomplishments are discussed. Written documentation is maintained of the matters addressed at such meetings.

11. The governing Board has established an Audit Committee or equivalent that is responsible for engaging the auditor, and ensuring that audit findings and recommendations are adequately addressed.
Overall Objective

Ongoing monitoring occurs in the ordinary course of operations, and includes regular management and supervisory activities, and other actions personnel take in performing their duties that assess the quality of internal control system performance.

Specific Objectives

1. Operating management obtains evidence that the system of internal control continues to function through independent reconciliations and management review of reports.

2. Communications from external parties corroborate internally generated information or indicate problems.

3. Appropriate organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.

4. Physical assets are examined periodically and compared to data recorded by information systems.

5. Irregularities and deficiencies, once identified, are promptly and effectively corrected.

6. The governing Board reviews and monitors audit findings and assess the adequacy of corrective action plans.


Appendix 1

Commonwealth of Massachusetts
Office of the State Comptroller:
Internal Control Legislation

Chapter 647 of the Acts of 1989

Chapter 647   THE COMMONWEALTH OF MASSACHUSETTS

In the Year One Thousand Nine Hundred and Eighty-nine

AN ACT RELATIVE TO IMPROVING THE INTERNAL CONTROLS WITHIN STATE AGENCIES.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

Notwithstanding any general or special law to the contrary, the following internal control standards shall define the minimum level of quality acceptable for internal control systems in operation throughout the various state agencies and departments and shall constitute the criteria against which such internal control systems will be evaluated. Internal control systems for the various state agencies and departments of the commonwealth shall be developed in accordance with internal control guidelines established by the office of the comptroller.

(A) Internal control systems of the agency are to be clearly documented and readily available for examination. Objectives for each of these standards are to be identified or developed for each agency activity and are to be logical; applicable and complete. Documentation of the agency's internal control systems should include (1) internal control procedures, (2) internal control accountability systems and (3), identification of the operating cycles. Documentation of the agency's internal control systems should appear in management directives, administrative policy, and accounting policies, procedures and manuals.

(B) All transactions and other significant events are to be promptly recorded, clearly documented and properly classified. Documentation of a transaction or event should include the entire process or life cycle of the transaction or event, including (1) the initiation or authorization of the transaction or event, (2) all aspects of the transaction while in process and (3), the final classification in summary records.

(C) Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority. Authorizations should be clearly communicated to managers and employees and should include the specific conditions and terms under which authorizations are to be made.
Appendix 1

Commonwealth of Massachusetts
Office of the State Comptroller:
Internal Control Legislation

Chapter 647 of the Acts of 1989

(D) Key duties and responsibilities including (1) authorizing, approving, and recording transactions, (2) issuing and receiving assets, (3) making payments and (4), reviewing or auditing transactions, should be assigned systematically to a number of individuals to insure that effective checks and balances exist.

(E) Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved. The duties of the supervisor in carrying out this responsibility shall include (1) clearly communicating the duties, responsibilities and accountabilities assigned to each staff member, (2) systematically reviewing each member's work to the extent necessary and (3), approving work at critical points to ensure that work flows as intended.

(F) Access to resources and records is to be limited to authorized individuals as determined by the agency head. Restrictions on access to resources will depend upon the vulnerability of the resource and the perceived risk of loss, both of which shall be periodically assessed. The agency head shall be responsible for maintaining accountability for the custody and use of resources and shall assign qualified individuals for that purpose. Periodic comparison shall be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts. The vulnerability and value of the agency resources shall determine the frequency of this comparison.

Within each agency there shall be an official, equivalent in title or rank to an assistant or deputy to the department head, whose responsibility, in addition to his regularly assigned duties, shall be to ensure that the agency has written documentation of its internal accounting and administrative control system on file. Said official shall, annually, or more often as conditions warrant, evaluate the effectiveness of the agency's internal control system and establish and implement changes necessary to ensure the continued integrity of the system. Said official shall in the performance of his duties ensure that: (1) the documentation of all internal control systems is readily available for examination by the comptroller, the secretary of administration and finance and the state auditor, (2) the results of audits and recommendations to improve departmental internal controls are promptly evaluated by the agency management, (3) timely and appropriate corrective actions are effected by the agency management in response to an audit and (4), all actions determined by the agency management as necessary to correct or otherwise resolve matters will be addressed by the agency in their budgetary request to the general court.
Appendix 1

Commonwealth of Massachusetts
Office of the State Comptroller:

Internal Control Legislation

Chapter 647 of the Acts of 1989

All unaccounted for variances, losses, shortages or thefts of funds or property shall be immediately reported to the state auditor's office, who shall review the matter to determine the amount involved which shall be reported to appropriate management and law enforcement officials. Said auditor shall also determine the internal control weakness that contributed to or caused the condition. Said auditor shall then make recommendations to the agency official overseeing the internal control system and other appropriate management officials. The recommendations of said auditor shall address the correction of the conditions found and the necessary internal control policies and procedures that must be modified. The agency oversight official and the appropriate management officials shall immediately implement policies and procedures necessary to prevent a recurrence of the problems identified.


Passed to be enacted, George Keverian, Speaker.

In Senate, December 22, 1989.

Passed to be enacted, William M. Bulger, President.


Approved,

Michael Dukakis

Governor.

Copyright 1998 Office of the Massachusetts State Comptroller; all rights reserved
Chapter 647 of the Acts of 1989 - Report on Unaccounted for Variances, Losses, Shortages, or Thefts of Funds or Property

TO: Agency Heads

FROM: Robert A. Powilatis, Deputy for Auditor and Investigative Services

DATE: January 18, 1996

RE: Law Relative to Improving the Internal Controls Within State Agencies

Chapter 647 of the Acts of 1989 was passed on January 3, 1990 and became effective on April 3, 1990. The law establishes the minimum level of quality acceptable for internal control systems for state agencies of the Commonwealth. Internal control systems for state agencies should be developed in accordance with internal control guidelines established by the Office of the State Comptroller. We will review compliance with the law during our audit engagements.

This law also requires that all unaccounted for variances, losses, shortages or thefts of funds or property be immediately reported to the Office of the State Auditor (OSA). The OSA is required to determine the amount involved and the internal control weaknesses that contributed to or caused the condition, make recommendations for corrective action, and make referrals to appropriate law enforcement officials. In order to comply with this law, we are requesting that all unaccounted for variances, losses, shortages or theft of funds or property be reported immediately to the OSA on the attached form.

Should you have any questions or desire additional information, please contact Howard Olsher, Director of State Audits at (617) 727-6200 (x25).

Attachments
Appendix 2

Report on Unaccounted for Variances, Losses Shortages, or Thefts of Funds or Property

TO: 

FROM: 

DATE: 

Agency: 

Address: 

Agency Contact Person (Name, Title, and Telephone Number): 

Date Detected: 

Explanation of Condition: 

Cause of Condition: 

Amount of Funds Involved: 

Appropriation Accounts, Trust Funds, Checking Accounts, etc. Involved (List all the particulars i.e., account numbers, banks, amounts etc.): 

Agency Division or Section Involved: 

Individual(s) Aware of Incident: 

No. of Individuals Having Access to Accounts/Funds Affected: 

Other Pertinent Information: 

Report Completed By: 
(Name, Title, and Telephone Number) 

Send the Report to: Office of the State Auditor, One Ashburton Place, Room 1819, Boston, MA 02108, Attn: Howard Olsher, Director of State Audits Office (617) 727-6200, Ext. 25 FAX (617) 727-5891.
Appendix 3

MISSION STATEMENTS
As approved by the Board of Higher Education
June 7, 1999

Public Higher Education System Mission Statement
The public University and university System in the Commonwealth of Massachusetts comprises fifteen community Universitys, nine state Universitys and the five campuses of the University of Massachusetts. The System exists to provide accessible, affordable, relevant and rigorous academic programs that adapt to meet changing individual and societal needs for education and employment. All campuses are committed to operating effectively and efficiently in order to maintain tuition and fees at a level as low as possible, while providing a high-quality education to every student who qualifies for admission. The public System is committed to continuous improvement and accountability in all aspects of teaching and learning. The Board of Higher Education and institutional Boards of Trustees recognize their responsibilities to the taxpayers and residents of Massachusetts in the performance of their roles and responsibilities. Massachusetts public higher education is a System with a distinguished past, increasing pride and unlimited potential.

Mission Statement for the University of Massachusetts
The University's mission is to provide an affordable education of high quality and conduct programs of research and public service that advance our knowledge and improve the lives of the people of the Commonwealth.
"...it is for life, not only for a living, that we must prepare our students." -William M. Bulger, President

Strategic Priorities of the University of Massachusetts
1) The University shall maintain the highest standard of academic excellence. The University of Massachusetts shall provide a quality, affordable university education to the citizens of the Commonwealth. The University shall strive to serve all qualified students regardless of their economic means. The University shall pursue distinction in its research and scholarship.

2) The University shall maintain an atmosphere where each person, regardless of religious, ethnic, economic or social background, will be comfortable. The University shall enroll and employ a diverse community of people.

3) The University shall offer and promote distinctive forms of public service. The University of Massachusetts shall provide the state with policy research, programs, and leadership to address public needs. The University shall support efforts to improve primary and secondary education and shall expand its continuing education programs to encourage lifelong learning. The University shall continue to promote the economic development of the state and its regions.
Appendix 3

MISSION STATEMENTS

As approved by the Board of Higher Education
June 7, 1999

4) **The University shall develop and manage its resources effectively.** The University shall wisely manage existing resources and aggressively develop new sources of revenue to meet operating and capital needs.

5) **The University shall demonstrate the excellence and advance the unique missions of its five campuses.** The University shall encourage its five campuses to pursue with distinction their respective strengths and strive to serve the best interests of their communities.

**Campus Vision**

Drawing from the vision statement for the entire University of Massachusetts, UMass Dartmouth developed a campus vision statement in 1992 placing emphasis on a special relationship between undergraduate and graduate education. Here's that statement:

The University of Massachusetts Dartmouth distinguishes itself by providing an intimate academic environment where the scholarly research and creative activities of faculty and graduate students are interwoven with the undergraduate experience. More than a regional university, the Dartmouth campus offers programs of educational excellence to undergraduate and graduate students from throughout the Commonwealth and beyond. While its academically distinguished faculty engage in professional activities of national and international scope, the campus has long been committed to economic development and has been a catalyst for regional initiatives. The university will continue its commitments to education and public service while expanding research efforts, establishing additional graduate programs, and addressing the educational needs of the state's increasingly diverse population. Its mission will reflect the University's in the following ways:

**Access**—Providing, within a personalized setting, a wide range of high quality baccalaureate and masters programs and selected doctoral programs; meeting the full financial need, as defined by standard measures, of all qualified applicants; strengthening student outreach efforts and collaboration with schools and community universities; encouraging and supporting the educational aspirations of under-represented student populations, thereby increasing the diversity of the campus community; easing transfer among institutions; and offering flexible programs for working adults.

**Excellence**—Offering intellectually challenging undergraduate and graduate programs that meet both individual student needs and those of the state; offering solid liberal arts curricula, for their own sake and as a foundation for professional programs; obtaining and maintaining national program accreditation where applicable; exposing students to new ideas and developments in their fields through close interaction with faculty; and building distinctive doctoral programs where research strengths exist and where special resources and needs are identified, such as the coastal marine environment, and including joint programs with other UMass campuses.
Appendix 3

MISSION STATEMENTS
As approved by the Board of Higher Education
June 7, 1999

**Innovation**-Enabling undergraduate and graduate students to experience the creation and application of new knowledge by expanding opportunities for them to participate in faculty research on campus and internships at nearby public and private organizations, thereby enriching students' education and aiding development in the region; continuing to create innovative interdisciplinary courses and degree programs, such as project-driven courses and community-based collaborative projects in health, education and the social sciences; and placing increased emphasis on a holistic approach to the undergraduate experience.

**Economic Development and Global Competitiveness**-Modernizing undergraduate and graduate education and supporting economic development by more closely linking liberal and professional education with the workplace, so that students can better integrate and apply their knowledge as they learn; providing research and technology transfer to marine and environmental industries; and providing research assistance and consultation to business, labor, government, health care and social service organizations.

**Public Service**-Improving the effectiveness of elementary and secondary education through collaborative undergraduate and graduate teacher education and in-service programs; adding cultural dimension to the lives of citizens through exhibitions and performances in the visual and performing arts; and providing support to businesses, human services organizations, and municipalities through research and policy analysis, student internships, forums, training assistance, and community-based programs.

**Quality of Life**-Enhancing and supporting the quality of life for individuals within a culturally diverse university community and for the citizens of the region by providing university-level library resources, distinguished programs in the visual and creative arts, and an accessible, stimulating intellectual environment; celebrating the cultural and linguistic richness of the area in studies and events; hosting eminent scholarly forums; and building a university community that fosters personal development, respect for the individual and cultural diversity of others and responsible citizenship.
Department-wide Risk Assessment

Department: University of Massachusetts System
Date / Version: September 30, 2002 Ver. 1
Submitted by: (University Controller or SWL)

High Level Department-wide Risk Assessment Approach:

The University performed an analysis on the potential risks that could hinder our defined mission and prevent us from reaching our goals. This analysis and identification of the most serious risks is a very high-level study and was completed by senior management of the University’s President’s Office. Senior management has considered the likelihood and significance of each risk noted and what steps need to be in place to either eliminate or minimize the risk to an acceptable level. This analysis is also an integral part of our internal control plan.

Mission Statement:

The mission of the University of Massachusetts is to provide a high quality education at the bachelor, masters and doctoral levels. Additionally the University as the State’s only research institution is heavily committed to a program of excellent research and public service. Through such programs we contribute to the economic viability of the State and we produce thoughtful and educated citizens for the work force and for the overall good of the State’s community. We encourage a diverse faculty and student body to assure that we have the best minds possible to enhance the education and research activity of the University. We are most competitive at the graduate education and research level and accept students from throughout the world.

Through varied approaches we are assuring that the learning experience for our students is of the highest caliber. Through Online course offerings and the latest equipment and telecommunication medium we are complimenting the traditional learning environment.

Through a broad based capital and operating budget process efforts are made to assure that the University is a good steward of the resources entrusted to its use. All management activity is conducted with the highest standards of professionalism and ethics. A regular and ongoing system of performance measurement allows university leaders and external stakeholders the opportunity to track successes and identify areas in need of improvement.

The Trustees, voluntary citizens appointed by the Governor, and the University President are ultimately responsible for the overall integrity and quality of the University of Massachusetts. Their efforts assure that the faculty and staff can make the most effective contribution to the life of the University of Massachusetts. All assets the faculty, the buildings and the other tangible and intangible assets must function in an atmosphere of respect and support.
Potential Risk Areas and Our Analysis

**Fraud against the University** – the University has recognized that financial fraud is a likely occurrence in any workplace environment and has taken steps to address these situations. A policy was approved by our Board of Trustees and distributed to all employees. Formal and clear guidance on reporting protocol, management responsibilities, and investigative responsibilities have been written.

**Loss of federal/state student financial aid eligibility** – Each of the University campuses administers both state and federal financial aid to their eligible students. Annual audits are performed that ensure that each of the campuses is compliant with the rules governing the administration of such funds. It is imperative that such funds are available to our students. Loss of federal or state financial aid would be detrimental to the student population across the University.

**Qualified financial opinion from external auditors** – The University of Massachusetts is audited annually by an external accounting firm. The University has never received a qualified opinion to date. An unqualified opinion is required in order to maintain debt covenants and other contractual agreements. Furthermore, as a material component of the Commonwealth of Massachusetts, the University’s receipt of a qualified opinion would not only have a significant impact on the University but also on the Commonwealth.

**Failure to maintain compliance with federal and state regulations, risking loss of research funding** - The University of Massachusetts is audited annually by an external accounting firm. One of the audits performed by this firm is to test compliance with our federal funds administration. Another audit focuses specifically on state financial aid programs. The General Purpose Financial Audit takes into account all other funds and incorporates the other mentioned audits. If for any reason, significant compliance breaches are discovered, restitution must be fulfilled or the funds will be returned and/or possible fines assessed. One of the critical missions of the University is research and therefore loss of such funds would have a detrimental impact on maintaining our mission. There is also a reliance on research funds to recover some indirect costs from such activities and to further our academic purpose.

**Accreditation** - Each of the 5 University campuses with their unique programs, mission and history are accredited on a regular basis. It is imperative that such accreditations be maintained. Loss of federal funds would be the most direct result with the loss of accreditation but loss of reputation for high standards would also result. The University campuses are all accredited by the Northeast association of colleges and universities and the various schools and colleges within the University are accredited by their specialty area.

**Student Quality** – The University sets standards for admission and adheres to them in very objective and set ways. Through high school transcript review and national standardized tests the University can be assured of a quality enrollment. The standards for admission have been steadily improving over the last ten years and are expected to continue to improve.
**Student Demand and Success** – In addition to the indicators of student quality noted above, enrollment trends, admissions indicators and student retention and graduation progress are all closely tracked by the University. These measures when stable and strong show a university that is providing a high quality, competitive academic program.

**Academic Reputation and Competitive Position** - An institution’s academic reputation is hard to quantify. However, attracting and retaining a high-quality productive faculty does resonate positively throughout the industry. Regular analysis of University measures of research productivity, student demand and success, and financial health to peer institutions helps management to gauge how well we are doing relative to our competition.

**Financial Health and Performance** – The University’s financial strength is directly linked to management decisions and demand for the educational program. Therefore, budget planning and financial performance measurement are key to the long-term health and vitality of the academic and research program of the University. The Board of Trustees annually reviews the University’s five year financial and capital plans and sets financial performance targets. External audits and bond rating agencies provide an additional level of objective review in this area.

**Research fraud** – Continuing monitoring of research activity must be conducted to both assure that no human subjects are being jeopardized and to assure that results are not being compromised. All campuses have the appropriate structure in place to monitor such standards of research activity. In addition, granting agencies and the peer review/journal review process set rigorous external quality control and compliance demands standards that university researchers must adhere to.

**Condition of Facilities** - The University is committed to maintaining and upgrading its capital assets so facilities and infrastructure does not degrade and fall into disrepair. The University relies on a combination of funding sources: state bond funds, UMBA/HEFA financing and its own operations to meet its capital needs. Loss of such funding to maintain the physical plant would put the University risk of failing to comply with regulations and mandates such as health and safety, ADA and environment. This lack of compliance could significantly hamper the learning environment and, at worst, could lead to the closing of buildings.

**Housing** - The University is dependent on a steady stream of funds to maintain and upgrade its residence halls. The majority of funds for such upgrades and repair come from student fees. A significant drop in enrollment of students choosing to live on campus would have a major impact on the ability of the University to provide capital improvements of residence halls.

**Failure to attract and retain quality faculty and staff** – The University depends on the quality and dedication of its workforce to meet its mission of teaching, research and public service. It is critical therefore that our wages and benefits are competitive and the work environment safe and supportive. The current fiscal challenges, including the unfunded status of collective bargaining agreements and the disruptions caused by the early retirement program have strained the work environment.
**Early Retirement Incentive Program (ERIP).** In December, 2001, the State Legislature enacted an Early Retirement incentive Program (ERIP). A total of 857 university employees, including more than 240 faculty, retired under this program. This presents significant risks and challenges for the University, which must service its student population and meet its business needs with a substantially diminished workforce.

The University will be hard-pressed in the short term to replace the skill sets of the retired employees and this will put additional pressures on the remaining staff. Moreover, because the University did not know until June which employees would in fact retire, it was unable in many instances to initiate the search procedures necessary to fill critical vacancies, particularly on the faculty side, in time for the current academic year. The University will therefore need to resort to alternative staffing strategies, including increased usage of part-time and/or temporary personnel.

**Information Technology Security and Access** - As with all other organizations, the University of Massachusetts is reassessing its IT security risk in the wake of the events of September 11, 2001. A key component of information security is assuring that only individuals who are authorized to have access to certain applications, information systems, and/or databases are appropriately authenticated and then granted access. The University is currently assessing its central systems vulnerability, its wide area network and information infrastructure. The review will provide an up-to-date IT security risk profile and a risk mitigation plan to permit the University to close any identified security gaps.

**Disaster Recovery Planning** – The technical infrastructure in place for the University’s centralized administrative and financial systems environment is designed to provide high system availability and recoverability in the event of hardware/infrastructure failures. An external project quality review team rated the University high and prepared. The objective of the high availability design is to limit system, network, and database down time to be no greater than the acceptable limits of the A&F business community.

The University has implemented industry standard recommendations for operational services of backup and restores ability. All environments are backed up according to schedule and production has nightly pre and post batch processing backups. Additionally system backups are stored off site, based on a monthly cycle in the event they are needed to help recover from a more catastrophic failure.

**Business Resumption Planning** – Each of the business units (campuses) is required to maintain basic downtime procedures in the event of scheduled or unscheduled downtime (Type One business recovery). In addition, the University’s high availability and redundant infrastructure allows for a high degree of confidence in our ability to recover data and avoid manual rework from a Type Two event.

In the unlikely event we were to ever have a catastrophic type event (Type Three) where there was a loss of the data center or the University’s WAN for an extend period of time, the University could resort to a number of situations, e.g. one, relocation of staff if a campus was inaccessible; two manual mode processes to manage check printing etc. At this time the University does not have a hot site situation for redundant and/or mirrored services outside the data center, but is working on additional options and alternatives.
NCAA violations and accreditation - The University of Massachusetts has a very broad range of athletic programs participating in up to 22 different varsity level sports for men and women. We participate in Division 1 to Division 3 sports at our campuses. Each campus takes all steps necessary to fully evaluate and comply with all NCAA rules. Each campus has taken responsibility for compliance by creating NCAA compliance officer positions that are responsible for adherence to published rules.

The University places special importance on the impact of athletics on the participant rather than on the spectator. Student athletes receive the same treatment as other students. They receive no special privileges, nor are they denied the rights and opportunities that would be available to them as non-athletes.

Sports for men and women receive equal emphasis and the desired quality of competition is similar in all sports.
Policy:

Responsibilities for budget preparation, adoption, execution, and reporting are segregated.

Procedures:

Responsible Person:

Associate Vice Chancellor for Finance

Budget Preparation:

All activities for the campus are budgeted including state appropriation, student fees, auxiliary enterprises (housing, dining, campus center, campus store, child care center, health services, UMass pass, and conferencing), Continuing Education, Fundraising for clubs and organizations, interest income, commissions and Restricted Funds including financial aid, grants and contracts, and gifts.

REVENUES

The budget is built by developing prudent revenue estimates that set the boundaries of expenditures. The revenue budget is built on reasonable estimates of enrollment provided by the Provost in consultation with the enrollment management team including housing occupancy and resident dining participation. The enrollment numbers are projected for the year, including an evaluation of second semester attrition and cover both the day and evening division for undergraduate and graduate students. Using these projections, a budget is built for each fund and combined to produce a total University budget. In addition, the state appropriation is projected utilizing historical and current data provided by the President’s Office. Auxiliary revenues projections consider enrollment as well as rate increases approved by the Board of Trustees or President.

EXPENSES

The expense budget is built utilizing previous year activity and individual budget hearings/meetings with each Vice Chancellor and the respective Deans and Directors. In preparation for these meetings, Administrative and Fiscal Services Division prepares preliminary budgets, which include any known commitments, annualizations from prior year decisions, and a preliminary copy of the Goldbook. The Goldbook is a budget management tool, which establishes personnel costs for the current. It also is the basis for personnel cost in the subsequent year. Listed below is the process to be followed for the budget/meeting process:
BUDGET MEETINGS/HEARINGS GUIDELINES

Guidelines for fiscal year budget hearings

Materials to be provided by A&F

1) Fiscal year Preliminary Working Goldbook
2) Prior Fiscal Year Final Budget Allocations
3) Enrollment Summary for Fiscal Years
4) Annualizations of Fiscal Year Opening Goldbook

Each Vice Chancellor, Dean, Director is required to submit one week in advance of their respective budget hearing the following materials:

1) Fiscal projected changes in personnel (both full and part time)
2) Fiscal Year projected changes in operating budget
3) Annualizations Related to Funding that was not in the Fiscal Year Opening Goldbook
4) Fiscal Year Budget Narrative responding to the following questions:
   a. What are the major issues facing your area?
   b. Are there any one-time purchases (i.e., equipment) in your fiscal year budget?
   c. Do you plan to make any one-time purchases in your fiscal year budget?
   d. How does your budget request meet expectations from the Chancellor as well as direct resources to meet objectives described in the Universities Strategic Plan?

BUDGET MEETINGS/HEARINGS

Prior to budget hearings, Vice Chancellor for Administrative & Fiscal Services and the Associate Vice Chancellor for Finance meet with the Chancellor and Assistant Chancellor to discuss specific issues Chancellor may have regarding the budget. Chancellor will indicate to each Vice Chancellor concerns/issues to be addressed in their area.

Vice Chancellor for Administrative & Fiscal Services, Associate Vice Chancellor for Finance and the Assistant Chancellor would conduct budget hearings with the following:

ACADEMIC AFFAIRS:
   Dean of Arts & Sciences
   Dean of College of Visual & Performing Arts
   Dean of Engineering
   Dean of Nursing
UNIVERSITY OF MASSACHUSETTS
Dartmouth Campus

Policies and Procedures
Budget

Dean of Charlton School of Business
Dean of SMAST
Enrollment Management
Continuing Education
Provost and Vice Chancellor for Academic Affairs (all other areas and general overview of area priorities)

STUDENT AFFAIRS
   Housing
   Campus Services
   Public Safety
   Vice Chancellor for Student Affairs (all other and general overview of area priorities)

UNIVERSITY RELATIONS
   News & Publications
   Center for Policy Analysis
   Vice Chancellor for University Relations (all other areas and general overview of area priorities)

LIBRARY SERVICES AND INFORMATION TECHNOLOGY
   PeopleSoft
   Library
   CITS

VICE CHANCELLOR FOR ADMINISTRATIVE & FISCAL SERVICES
   Facilities
   Human Resources
   Administrative Services
   Associate Vice Chancellor for Finance (all other areas and general overview of area priorities)

CHANCELLOR
   AA/EEO
   Chancellor, Assistant Chancellor (all other areas and general overview of area priorities)

A&F develops an Executive Summary of all areas to be reviewed with Chancellor and shared with Executive Staff. Chancellor may request additional information from each Vice Chancellor regarding information from budget hearings. Follow-up and final summaries are handled by A&F and reported back to Chancellor.

Chancellor makes preliminary allocations, which will be finalized after legislative action.
Preliminary allocations will be sent to each Vice Chancellor. Vice Chancellors are encouraged to meet with members of Administrative and Fiscal Services to review preliminary allocations. Each Vice Chancellor will submit back to Administrative and Fiscal Services no later than 2 weeks after receiving their preliminary budgets sub-allocations to their respective departments. The Budget Office will load budgets into the PeopleSoft Financial System. Once loaded, a reconciliation of the preliminary budget and the PeopleSoft Financial System is done. Chancellor makes preliminary allocations final after legislative action.

Budgets are not controlled at the subsidiary level with the exception of the following: payroll, fringe, utilities, and debt service or lease payments. All other budgets are pooled. Expenditures however, are recorded at the object code or account level.

BUDGET REPORTING

There are both internal and external budget reports used by the University to manage its resources. External reports include the Operating Budget, Mid-Year Budget to Actual Report, Board of Higher Education Fiscal Data Worksheet, Fee and Revenue Budgets, Capital Expenditure Budgets, Capital Adaptation and Renewal Report, Financial Indicator Report for the Performance Measurement System, and State Spending Plan. Internal budget reports include Revenue Projection Budget, Expense Projection Budget, State Maintenance Budget, Goldbook, Executive Level Allocation Worksheet, Monthly Departmental Budget to Actual Report, and Statement of Revenues and Expenses. Various groups to ensure actual activity is consistent with budgeted activity use these various reports. In addition, budget managers have the capability to query pieces of information from the PeopleSoft Financial System that assist them in making day-to-day decisions. The Budget Office analyzes activity throughout the year and brings forth issues with the appropriate budget manager as the may arise.

GOLDBOOK

The Goldbook is a budget management tool used track personnel expenditures from year to year. Preliminary Goldbooks are prepared to assist Vice Chancellors with budget preparation. Official Opening Goldbooks will be distributed when the budget process is complete. The following is included in the Official Opening Goldbook:

- All employees currently on the payroll
- Vacant positions approved through the budget process for that fiscal year
- Annualizations from prior year approved positions

Each month, Vice Chancellors will receive an updated Goldbook. This update will include any and all changes. In addition, each Vice Chancellor will receive a Reserve
Page worksheet. The Reserve Page Worksheet is provided to help each Vice Chancellor track coming and going activities to show funds that are freed up and new obligations incurred. Available funds may be used for one-time purchases only with the prior approval of the Vice Chancellor for Administrative and Fiscal Services. Funds that remain freed up after April 15th shall revert to a central pool.

BUDGET MODIFICATIONS

Budgets are allocated at the Vice Chancellor level. Each Vice Chancellor is responsible for monitoring their respective departmental budget activity. In general, individual departments may overspend their allocation as long as the overall divisional budget has sufficient funds. Transfers within a division can be made by e-mail to the Budget Office, Janice Fiola. These types of transfers require approval from the individual who has budget authority from where the funds are being transferred from. Transfers must be made from and to the same fund source. That is, CSF funds may only be transferred to other CSF accounts. Transfers of this nature, which do no create a change to the overall budget are routine and will be processed within 3 days of receipt of the e-mail.

Request for budget modifications that increase the original budget must be approved by the Vice Chancellor for Administrative and Fiscal Services. Modifications of this type will undergo extreme scrutiny. Any such request should be submitted in writing to the Vice Chancellor for Administrative and Fiscal Services justifying the request.

Budget modifications that request moving payroll, fringe, utilities, and debt service or lease payments must be approved by the Vice Chancellor for Administrative and Fiscal Services. Modifications of this type will undergo extreme scrutiny. Any such request should be submitted in writing to the Vice Chancellor for Administrative and Fiscal Services justifying the request.

Vice Chancellors, Deans, Directors, and Department Chairs are responsible that within their administrative units; all proposed expenditures are consistent with University policies and federal and state regulations, and adequate funds have been budgeted to support programs and operations.

BUDGET CALENDAR

Below is the format for a typical fiscal year budget calendar.
Activity:
Chancellor and Provost commit to faculty searches for fall 20XX

Responsible Person:
Provost

Due Date:
October

Activity:
A rolling five fiscal year enrollment projection by class (FTE & Headcount, Day, DCE, Graduate and Undergraduate) including Housing (by room type) and Dining (by meal plan).

Responsible Person:
Provost

Due Date:
October 31, 20XX

Activity:
Board of Trustee approval of Room & Board Rates

Responsible Person:
Associate Vice Chancellor for Finance

Due Date:
January

Activity:
Preliminary Revenue Projections including State Appropriation, Student Fees and Auxiliaries

Responsible Person:
Associate Vice Chancellor for Finance

Due Date:
Early November

Activity:
Budget Review Board Meeting

**Responsible Person:**
Vice Chancellor for A&F

**Due Date:**
Mid-November

**Activity:**
Preliminary working fiscal year 20XX Goldbook distributed to Vice Chancellors

**Responsible Person:**
Associate Vice Chancellor for Finance

**Due Date:**
Late November

**Activity:**
Guidelines for fiscal year 20XX budget hearings distributed to Vice Chancellors

**Responsible Person:**
Associate Vice Chancellor for Finance

**Due Date:**
Late November

**Activity:**
Fiscal Year 20XX budget hearings with Chancellor, Associate/Assistant Chancellors, Vice Chancellors, Associate/Assistant Vice Chancellors, Deans, Division Heads

**Responsible Person:**
Associate Vice Chancellor for Finance

**Due Date:**
December through February

**Activity:**
Budget Review Board Meeting
Responsible Person:
Vice Chancellor for A&F

Due Date:
December

Activity:
Governor’s House I Budget

Responsible Person:
President’s Office

Due Date:
January

Activity:
Vice Chancellors and Executive Staff meeting to show fiscal year 20XX revenue and expense assumptions

Responsible Person:
Vice Chancellor for A&F and Associate Vice Chancellor for Finance

Due Date:
Late February

Activity:
Mandatory and Nonmandatory Fee Rates submission

Responsible Person:
Associate Vice Chancellor for Finance

Due Date:
March

Activity:
Distribute fiscal year 20XX Preliminary Budget to Vice Chancellors

Responsible Person:
Associate Vice Chancellor for Finance
Due Date: Mid-March

Activity:
Vice Chancellors review and comment on fiscal year 20XX Preliminary Budget

Responsible Person:
Vice Chancellors

Due Date: Late March

Activity:
Final fiscal year 20XX Opening Goldbook and budget distributed to Vice Chancellors

Responsible Person:
Chancellor/Vice Chancellor for A&F

Due Date: Mid-April

Activity:
Budget Review Board Meeting

Responsible Person:
Vice Chancellor for A&F

Due Date: Mid-April

Activity:
House and Senate version of budget released

Responsible Person:
President’s Office

Due Date: April-May
Activity:
Conference Committee version of budget released

Responsible Person:
President’s Office

Due Date:
May-July

Activity:
Final President’s Office Allocation to Campus

Responsible Person:
President’s Office

Due Date:
July-September

Activity:
Budget Review Board Meeting

Responsible Person:
Vice Chancellor for A&F

Due Date:
September
Policy:

Receipts are accounted for and balanced to reported collections on a daily basis.

Procedures:

1. The Bursar’s Office is responsible for verification of receipts to reported collections.
2. Receipts are prepared for deposit by the deposit clerk.
3. The deposit clerk will also prepare the cash receipt for entry into the general ledger. (Note this is a temporary procedure during the conversion to PeopleSoft Financial Systems).
Policy:
Receipts are deposited intact on a daily basis.

Procedures:

1. The deposit clerk in the Bursar’s Office verifies receipts to reported collections and prepares the bank deposit for pickup by the courier service.
Policy:

Facilities exist for protecting undeposited cash receipts.

Procedures:

1. The Bursar’s Office provides a fireproof safe to store undeposited cash receipts.
UNIVERSITY OF MASSACHUSETTS
Dartmouth Campus

Policies and Procedures
Cash Receipts

Policy:

The responsibility for collecting, controlling, and depositing funds is segregated from maintaining accounting records.

Procedures:

1. The University Enrollment Center is responsible for collections on student accounts, including processing mail and credit card payments.
2. The Bursar’s Office is responsible for controlling and depositing funds.
3. General ledger postings relating to revenues and collections are generally accomplished through automated feeds generated by the Billing and Receivables System (BRS).
Policy:

Responsibilities for cash receipts are segregated from those for cash disbursements.

Procedures:

1. The Bursar’s Office is responsible for controlling and depositing cash receipts
2. The Purchasing and Accounts Payable Departments are responsible for the approval and disbursing of funds.
Policy:

Timely bank reconciliations are prepared and reviewed by someone independent of the cash receipts function.

Procedures:

1. All bank reconciliations are performed by the University Treasurer’s Office.
Fiscal Procedure – Imprest Checking Accounts

Subject

Imprest Checking Account Procedure Governing All Imprest Checking Accounts University-wide

Purpose

To provide an imprest checking account to facilitate payments authorized hereby and described under the Use of Funds Section. This checking account should not be used as a substitute for the payroll or disbursement systems. This checking account is provided to accommodate those extraordinary demands for payment that each campus must facilitate.

Policy

A. Authorization –

The Treasurer of the University of Massachusetts is authorized and empowered by the Board of Trustees to establish all bank accounts, to make deposits in and withdrawals from said accounts and to sign or endorse in the name of the University of Massachusetts or the Board of Trustees such official documents and vouchers, including checks, drafts, letters of credit and the like as require the signature of the financial officer of the University; and, he is authorized to designate personnel to sign or endorse checks for special program checking accounts both here and abroad (Doc. T97-014).

B. Authorized Signatures –

1. The Treasurer and Associate Treasurer shall be the primary signatories as authorized by the Board of Trustees.

C. Additional Signatories –

1. Additional signatories may be designated and approved by the University Treasurer or Associate Treasurer. Designated signatories will be noted via a copy of the signature card on file in the University Treasurer’s Office and attached hereto as Attachment A.

D. Authorized Amount –
1. The principal amount of any imprest checking account shall be recommended by the Vice Chancellor for Administration & Finance and approved by the University Treasurer.

2. No additions to or reductions of the checking account principal balance shall be made unless approved by an authorized official within the University Treasurer’s Office.

3. The principal amount of this checking account shall be recorded without exception in the accounting system.

E. Use of Funds –

1. Payments from this imprest checking account shall be for the convenience of the University in order to expedite the processing of payments.

2. Payments from the imprest account should be the option of last resort. Every effort should be made to process the transaction through the normal accounting or payroll process.

3. The maximum single payment drawn on this imprest checking account shall not exceed the current balance of the account.

4. Payments from the subject activity’s imprest checking account shall be governed by all procurement and payroll policies as applicable.

5. A senior campus fiscal officer will certify on a monthly basis adherence to the policy guidelines. Said certification will be in the form of a signature noted on the check register monthly and dated.

6. All expenditure activity originating from this account shall be recorded individually in the accounting system.

Listed below is a representative sample of the appropriate uses of the imprest account:

a. Payroll Advance
b. Payroll refund adjustments
c. Worker’s Compensation adjustments
d. Personal Advance
e. Vendor Payments
f. Emergency expenses specific to campus operations
g. Emergency expenses for health and safety remediation
h. Emergency expenses specific to student operations
i. Student excess award payments
j. Athletic entry fees and game day officials fees
k. Meal money
l. Emergency student or Resident loan
m. Coin & currency funding
n. Travel advance or allowance
Procedures

A. Checks/Check Register –

1. A pre-numbered check shall be used.

2. A check register shall be maintained wherein deposits for funding and reimbursement of expenditures are entered and individual checks drawn and recorded. The check register will be maintained in electronic format.

B. Expenditure Documentation –

1. Each payment from the subject imprest checking account must be supported by the appropriate level of documentation and recorded individually in to the University General Ledger System (Peoplesoft Financials).

2. Documents supporting checks written must be retained as justification for replenishment of the imprest checking account by the issuing department.

3. The imprest fund shall be reimbursed no less frequently than once a month but may be reimbursed more frequently as circumstances dictate.

C. Bank Reconciliation –

1. The reconciliation of the checking account is performed by the University Treasurer’s Office.

2. Monthly bank statements for the subject imprest checking account shall be sent directly to the University Treasurer’s Office by the bank. The fund custodian should send electronically a copy of the check register and copies of any deposit slips to the Treasurer’s Office by the 10th of the following month. If the fund custodian performs a reconciliation of the subject account, then a copy of the reconciliation should accompany the copies of the check register and deposit slips.

Definition of Terms

A. Imprest Account –

This is a checking account in which the principal amount to be accounted for does not change except as stated in Policy Section D.2. Any expenditure of the principal shall be reimbursed and the total principal kept intact at all times. The balance in the imprest account plus expenditures to be reimbursed must equal the principal to be accounted for.

Sanctions

Failure to observe this policy will subject the Campus to forfeiture of this checking account.
Policy for the Development and Administration of Grants, Contracts and Cooperative Agreements For Sponsored Programs

PURPOSE

This policy establishes principles essential for the sound management and administration of grants, contracts and cooperative agreements for sponsored University programs in instruction, research, and public service. They provide appropriate controls for the development of proposals and applications; procedures and criteria for the acceptance of grants and contracts for sponsored programs; and prudent and effective administrative and accounting controls for grant, contract and cooperative agreement administration. This policy assigns responsibility to organizationally separated offices and individuals for each step in the administrative process, addressing both pre- and post-award administration.

The University engages in a wide variety of programs, projects, and other activities, which are supported by funds from external agencies and organizations. Funds received for such programs are held in trust by the University and are separately budgeted and accounted for. The mechanisms used by external organizations to provide support are categorized into three types: Grants, Contracts and Cooperative Agreements.

The University's management procedures for the three general mechanisms are essentially the same. Each is treated by the University as a specification of obligations which may require separate accountability for expenditures and evidence of performance consistent with the intentions of the sponsor.

DEFINITIONS

A grant is an award to the University which does not require the production of specific results or services, but which typically defines objectives (either as proposed by the University or defined by the sponsor) toward which the award proceeds are to be applied. The grant award may be restricted as to where, by whom, and for what purposes the proceeds may be used.

Contracts are agreements between one or more sponsors and the University. The terms of the agreement outline very specific goals and requirements for goods and/or services to be provided by the University to the sponsor. It is routine for these goods or services to be provided on a specific schedule. The relationship between the sponsor and the University is one of procurement.

Cooperative agreements are basically bilateral grants, used when substantial sponsor involvement is anticipated in the management and/or performance of the sponsored activity.

APPLICATION

This policy supersedes existing policies and procedures for administration of sponsored programs. It applies to all grants, contracts and cooperative agreements for such programs and to all organizational units (e.g., colleges, schools, departments, centers, institutes, and programs) of the University and other affiliated organizations, wherever located. This policy does not apply to patient care contracts at the Worcester campus, which are governed by Trustee Documents T76-031C, Interagency Agreement and T78-081, Authorization of Chancellor to Execute Hospital Reimbursement Agreements with Blue Cross and/or its Successor.
UNIVERSITY OF MASSACHUSETTS
Dartmouth Campus

Policies and Procedures
Grants and Contracts

Any campus may institute additional policies and procedures that may be more, but not less, restrictive than the conditions of this policy.

ORGANIZATION

The office of the Vice President for Management and Fiscal Affairs shall have responsibility for University-wide conformance with this policy. The Chancellor or his/her designees shall have responsibility for campus-wide conformance with this policy. The campus officials for pre- and post-award administration of sponsored projects, the University Controller, and the Vice President for Management and Fiscal Affairs shall constitute the primary University system group, which establishes practices and procedures to implement this policy.

Each of the campuses will have an office for sponsored project administration reporting to an appropriate campus designated Vice Chancellor. The campus office for sponsored project administration shall provide administrative support services to campus researchers and directors of sponsored projects and, in collaboration with the campus fiscal services, shall effect conformance with University fiscal management practices.

ADMINISTRATIVE RESPONSIBILITIES

The campus sponsored project administrators and Controllers are assigned specific responsibility for pre- and post-award administration of grants, contracts and cooperative agreements. The sponsored project administrator at each campus is the sole authorized institutional official having authority for submitting proposals and applications to funding agencies.

Sponsored programs are essential and integral to research, and public service in the academic setting. A primary function of the office of sponsored project administration, therefore, is to support the University's principal investigators, both in their relationships with outside funding sources and in their dealings with other University administrative units.

Each office for sponsored project administration is responsible for initiating in collaboration with the campus fiscal services, campus procedures for pre-and post-award related activities. The procedures must be in accordance with all University-wide administrative policies which affect grant and contract management (e.g., Personnel, Purchasing, and Accounting). The sponsored project administrators and Campus Controllers shall serve as the formal point of contact between the campuses and funding agencies on administrative and financial matters.

The office for sponsored project administration shall participate in the preparation of annual studies related to research activities of the campus. The sponsored project administrator shall have the responsibility for final certification of project budgets and for determining whether amendments or revisions to project budgets shall be subject to the internal review procedures. Requests for changes which require prior approval shall be prepared by the principal investigator and endorsed by the sponsored project administrator. The principal investigator for a sponsored project shall be responsible for administering the project in conformance with the approved budget. The designation of principal investigator is to be determined by each campus in addition to describing the roles and responsibilities of the principal investigator or those designated. The Campus Controller shall not process disbursements on any account (except reimbursable contracts) unless funds are available or unless approval for transfer or advances has been given in accordance with the budgets and this policy; such approval is subject to review by the sponsored project administrator.

As a partner in sponsored project activities, it is the responsibility of the principal investigator to conduct the project consistent with all federal and state laws including the Massachusetts Conflict of Interest Law, Chapter 268A, all University policies, and with the highest ethical standards. In addition, the principal investigator will be responsible for the substantive conduct of the project, adherence to the terms and conditions, initiation of all
personnel and purchasing actions, disclosure of potential conflicts of interest, invention disclosure, and equipment inventory.

**ADMINISTRATIVE RESPONSIBILITIES**

**Pre-award**

Each campus will establish internal implementation procedures for sponsored project administration maintaining consistency with the policy of this document. These procedures must include the designation of individuals for campus programmatic and budgetary review and approval of proposed projects. In principle, every proposal must be approved by at least two higher organizational authorities with regard to appropriate University goals and resources. Normally, in the case of academic departments, the programmatic aspects of proposals must be approved first by the appropriate Chair (or equivalent) and then by the Dean of the School or College or his/her designee. This review should ensure that the proposal is consistent with the goals and objectives of the department, college or institution and should also assess the impact of the project upon the future resources of the organization and any changes in the level of institutional support which may result from the acceptance of an award. Prior to signing, the Chair and/or the Dean must confirm the availability of space, major technical resources and equipment, institutional support personnel, and must endorse commitments for cost sharing, matching funds, or any proposed retention of project-supported personnel after the expiration of the award. If such confirmations and endorsements cannot be made, the Chair or Dean should refer the proposal to other appropriate campus officials for resolution. If in a particular case the Chair and Dean are unable to review and approve a proposal, or to make the required commitments and endorsements as to resources and cost sharing, then such proposal must be approved by the Chancellor or his/her designee.

Programmatic and budgetary review of proposals generated by such organizational units as Institutes, Centers, and Programs shall be performed by the administrators to whom the unit head reports. Project proposals generated by Institutes, Centers, or Programs which report to administrators of the President's Office but that involve activities at any campus of the University, shall be reviewed by appropriate officials at that Campus prior to submission to the sponsor.

In the preparation and submission of proposals, the following provisions shall apply:

1. Proposals must conform with the policies of the Board of Trustees and of the University Administration.
2. The sponsored project administrator shall review and approve proposed contracts prior to their acceptance by the University. Legal review, when requested by the sponsored project administrator, shall be performed by the University Counsel or by designated Counsel in a timely manner.
3. An Internal Processing Form (IPF) shall accompany all proposals through the review process. This form shall summarize pertinent data from the proposal and provide signature lines for reviewers to register their approval.
4. Multi-campus proposals require review and approval of each campus' sponsored project administrator prior to submission.
5. The Vice President for Academic Affairs shall be informed at the time of submission of all proposals for projects which will have a pronounced impact upon the goals and programs of the University.
6. The Chancellor or his/her designee shall review and approve proposals which include University commitments for new permanent professional staff positions, matching funds in excess of $50,000, or substantial construction or renovation.
7. Transmission of all project proposals and acceptance of all awards from any sponsoring agency must have the signature of an authorized institutional representative.
Post-award

General

Inasmuch as the award is made to the University of Massachusetts, and not to an individual or a department, the University is legally responsible for the project and more importantly, for fulfilling the sponsor’s requirements.

It is the responsibility of the University Controller, in conjunction with the campus fiscal services to establish the controls necessary to assure sound fiscal management of sponsored agreements. Campus fiscal offices will coordinate all accounting and fiscal matters relating to sponsored agreements among campus administrative offices, research administrators, and principal investigators. If University fiscal policies are more restrictive than the terms and conditions of the sponsored agreement, University policies will take precedent over the sponsored agreement.

It is the responsibility of the principal investigator and the campus fiscal services to adhere to the fiscal terms and conditions of the sponsored agreement, comply with University and campus fiscal policies and procedures. The principal investigator shall be responsible for submitting technical, patent and other required scientific reports in a timely manner to both the sponsoring agency and the campus fiscal services.

Contract Terms

Campus fiscal offices are responsible for determining the credit worthiness of sponsors. Each campus will develop a procedure to use credit information as a determining factor in evaluating the sponsor. Whenever possible, partial payments from sponsors received in advance should be encouraged. Late fees should be charged when allowable under the terms of the sponsored agreement.

Establishing Accounts

The University Controller, in conjunction with campus fiscal offices, is responsible for the timely establishment of accounts in the University's financial systems in accordance with the term and conditions of the sponsored agreement. Campus fiscal offices should implement procedures that ensure accurate and timely reporting for each grant or contract and provide copies of these reports to the principal investigator on a timely basis.

Billings/Letters of Credit

It is the sole responsibility of the campus fiscal offices to prepare and submit, on a timely basis, any fiscal reports and billings to sponsors in accordance with terms and conditions of the agreement. All University billings, letters of credit or other requests for payment under grants, restricted gifts, and contracts for sponsored projects shall be in the name of the University of Massachusetts. Drawdowns under letters of credit shall be authorized by the University Treasurer or his/her designee.

Indirect Cost Rates

Each Chancellor or his/her designee shall negotiate the indirect cost rates applicable to projects supported by federal agencies and non-federal sponsors respectively on his/her campus. A copy of the approved rate agreement shall be sent to the President. These rates shall not be varied or waived without prior written approval of the appropriate office of sponsored project administration.
Collections

The campus fiscal offices shall institute procedures to maintain proper accounting and control of all cash receipts from sponsored agreements billings. Payments received on account for sponsored projects shall be deposited by the fiscal office designated to receive grant receipts in bank accounts established by the University Treasurer or his/her designee. Anyone receiving monies due the University shall immediately forward them to the designated campus fiscal office. Each campus shall implement collection procedures. A reserve for uncollectible accounts shall be established by each campus.

Expenditures

In a timely fashion, the campus fiscal offices shall review and approve all expenditures for compliance with sponsor requirements, University policies as outlined in Trustee Document T92-031, Policy for Management of University Funds and campus procedures. Signatures of employees, including temporary designees, authorized to approve expenditures shall be on file in the campus fiscal office. Authorizations for payments involving non-personnel expenditures require approval by the principal investigator. All personnel action forms require certification by the campus fiscal offices that funding is available. Personnel action forms for initial appointments and changes in compensation rates shall include the original signature of the principal investigator and the original signature of the Department Head or Dean. Other personnel action forms shall require only the principal investigator's signature. The campus fiscal offices shall provide advice and service to principal investigators to guide expenditures in a manner that assures maximum benefit and utilization of funds from sponsored agreements.

Recovery of Indirect Costs and Fringe Benefits

The campus fiscal offices will apply indirect cost rates and fringe benefit rates in accordance with federal and state regulations. The indirect cost rates are not to be varied or waived without prior written approval of the Chancellor or his/her designee upon recommendation of the campus office of sponsored projects administration.

Institutional Commitments

It is the policy of the University to generally cost share only the dollar value of contributed personnel time during a project period, together with the associated indirect costs, which is paid from State or other non-Federal funds. However, at certain times, and with permission of the institution-contracting officer, the University may cost share or match other costs as long as the costs are not included in the University's negotiated overhead rate. When this does occur, it is the responsibility of the principal investigator to maintain records of actual cost sharing expenditures.

In cases where a particular sponsor restricts the recovery of indirect costs by the University, the unrecovered portion of those costs may be shown in the project budget as cost sharing.

In instances where the cost sharing requirements of a sponsor are such that the University cost sharing from usual sources is insufficient, such as the need for matching funds, the principal investigator and the campus office of sponsored projects administration will prepare a statement of University participation.

Audit

Sponsored projects are subject to agency audit, State audit, and University internal and external audit.
Amendments

All changes in any sponsored project agreement, including time extensions, shall be by formal amendment requested in writing by the principal investigator and processed by the contracting officer. A copy of each change must be submitted to the campus fiscal services.

Subgrants and Subcontracts

These policies apply to all subgrants and subcontracts whether received or issued by the University.
Policy:

Grant disbursements are processed under the same degree of controls applicable to other transactions for the procurement and payment of goods and services.

Procedures:

Policy:

Procedures are modified when funds are disbursed under grant or loan agreements and related regulations impose requirements that differ from the entity’s normal policies.

Procedures:

1. Grants and Contracts are restricted funds and any expenditures must be related to the specific project, i.e., personnel, specific equipment purchases, etc. All expenses adhere to University requirements.

2. Make reference to relevant sections of policies and procedures relating to grants and contracts.
Policy:

Procedures and controls exist to provide reasonable assurance that only eligible individuals receive assistance under Federal award programs and that amounts provided to or on behalf of eligibles were calculated in accordance with program requirements.

Procedures:

1. The University has met all eligibility and certification requirements and has a current participation agreement with the Secretary for each of its student financial aid programs.

2. Procedures for determining student eligibility and disbursements to award recipients are prescribed in accordance with The Student Financial Aid Handbook and documented in the Student Financial Aid Control Procedures Manual.

3. The University coordinates Title IV programs with other Federal and non-Federal programs of student financial aid it administers to preclude the awarding of assistance in excess of students' financial needs.

4. Disbursements to award recipients are made according to prescribed procedures and within prescribed limits.

5. Refund calculations and overpayment determinations are made according to prescribed procedures.

6. Requests for/draw downs of Federal funds are limited to the University's immediate needs and are within the amount authorized for each program.

7. Responsibility for authorizing disbursement by awarding financial aid is independent of the disbursing function.
Policy:

Procedures and controls exist to provide reasonable assurance that the draw down of Federal cash is only for immediate needs.

Procedures:

1. The draw down of Federal cash is on a cost reimbursement basis.
2. The Director of Grant Accounting and the Grants Accountant have security authorization to draw down Federal funds on a cost reimbursement basis.
3. The draw down is requested at the beginning of each calendar month for the prior month and the tool used is the current monthly financial record for each account.
4. Any applicable indirect cost is calculated and added to the prior month expenditures and that total is requested from the granting agency.
5. At present, the agencies consist of the Department of Education, Office of Naval Research, National Science Foundation, National Aeronautic and Space Administration, National Oceanic and Atmospheric Administration, and the U.S. Department of Agriculture.
6. Online security has been established for the above employees and funds are requested and fed-wired into the Federal Clearing account of the University.
7. A memo is sent to the Bursar’s office stating what dollars have been requested and specific accounts for deposit.
8. When the funds have been received by the Bursar’s office, the Grant Accounting office is notified.
Policy:

Controls exist to provide reasonable assurance that Federal funds are used only during the authorized period of availability.

Procedures:

1. All sponsored agreements have a beginning and ending date.
2. All expenditures and time and effort must take place within the parameters of the project period.
3. Extensions must be requested in writing and approved by the funding agency.
4. When an award is made to the University, the Office of Grants and Contracts contacts the Office of Grant Accounting for an individual account number.
5. An account memo is generated by the Office of Grants and Contracts to the Principal Investigator, Department Chair, Dean and Director of Grant Accounting.
6. The award memo along with a copy of the agreement is forwarded to the Director of Grant Accounting for account setup in the financial system.
7. The Director of Grant Accounting establishes the general ledger, subsidiary ledger and enters the line item budget as approved by the funding agency.
8. An account folder is made and indirect cost information and billing information is recorded in the front of the folder.
9. The Director of Grant Accounting and, in her absence the Grant Accountant, reviews and signs all requests for purchase or reimbursement on each award including requests for salary or hire.
Controls exist to ensure that costs charged to grants are in compliance with grant agreements.

1. All awards have an approved line item budget indicating direct and indirect costs.
2. The Director of Grant Accounting or the Grants Accountant reviews all expenditures for allowable costs in accordance with Circular A-21 and those same costs are included in the approved line item budget.
3. The requests for expenditure, i.e., purchase orders, request for procard, travel reimbursements, hiring of consultants and employee reimbursement or hire are signed by the Director of Grant Accounting or the Grants Accountant.
Policy:

Procedures exist for obtaining grantor approval before incurring expenditures in excess of budgeted amounts or for unbudgeted expenditures.

Procedures:

1. Most Federal agencies grant the grantee-expanded authority to rebudget non-indirect cost generating line items between 10 and 20 percent. For example, lab supplies may be rebudgeted to office supplies or travel. An example of a change in salary lines may be from grad assistants to research assistants.

2. Any request to change salary to a non-indirect cost generating line such as equipment or supplies must be approved by the granting agency.

3. The Principal Investigator may contact the program manager directly or request that the Office of Grants and Contracts make the contact.

4. If approved, the Office of Grant Accounting is notified of the approved change and the Director will revise the budget in the accounting system.
Policy:

Procedures exist to identify, before order entry, costs and expenditures that are not allowable under grant programs.

Procedures:

1. All expenditure requests under sponsored agreements are reviewed and signed by the Director of Grant Accounting or the Grants Accountant to ensure costs are allowable in accordance with Circular A-21, are allowable under contract requirements, and have available budget.
Policy:

An indirect cost allocation plan is established and has been developed in accordance with grantor requirements and approved as required by the grantor.

Procedures:

1. The negotiated indirect cost rate is calculated every three years and is currently based on salaries and wages.
2. The University’s cognizant agency is Health and Human Services.
3. The Director of Grant Accounting performs the calculation in accordance with Circular A-21 guidelines (copy attached).
Policy:

Grant activity is accounted for so that it can be separated from the accounting for locally funded activities.

Procedures:

1. Accounts for sponsored awards are established in individual accounts with separate general ledgers and subsidiary ledgers in an account number range designating restricted funds.

2. Accounts are coded restricted and are differentiated from appropriated and trust fund accounts that are coded unrestricted. The Director of Grant Accounting establishes all restricted accounts in the University accounting system.
Policy:

Procedures exist to monitor compliance with grant requirements.

Procedures:

1. All sponsored agreements require monthly, quarterly, and final financial reporting, including any cost sharing or matching information. The Director of Grant Accounting and Grants Accountant shares these responsibilities.

2. The Principal Investigator performs performance reporting.

3. Intellectual Property and publication reporting is done at award closeout by the Office of Grants and Contracts, the original Contractor.
UNIVERSITY OF MASSACHUSETTS
Dartmouth Campus

Policies and Procedures
Grants and Contracts

Policy:

The level of authority for approving grants and contracts is appropriate.

Procedures:

All University requests to federal or state agencies, private foundations and corporations must be coordinated with the Office of Grants and Contracts (OGC). The following steps are required for submitting a grant or research proposal to an outside agency:

1. Develop your idea. Visit the OGC for information and assistance. We will help with searching for an appropriate funding agency, interpretation of application guidelines, budget preparation, and final review of the proposal.

2. Contact your Department Chairperson and College Dean to inform them of your project and project needs, i.e. release time, facilities, etc. Consulting with them in advance will help anticipate any difficulties in obtaining formal University approval.

3. Once a proposal has been typed and all application forms prepared, attach a UMASSD Internal Review and Transmittal Form and obtain appropriate signatures. Signatures of the Department Chair, College Dean and OGC are necessary before the University’s authorized official signs a proposal. This form is available in the OGC, your Department Chair’s office, your Dean's Office or can be accessed electronically on the OGC's home page. All proposals should arrive at the Office of Grants and Contracts five (5) business days prior to deadline/target date, so please anticipate the necessary time that will be needed to obtain approval from your Chair and Dean.

4. For proposals that entail the use of hazardous materials, procedures or study of humans and/or animals, you will need to obtain institutional approval from the designated committees. Please contact the OGC for assistance.

5. The Principal Investigator (PI) is responsible for obtaining the first three signatures on the Transmittal Form (his/her own as the PI, the Department Chairperson; and the College Dean). The original proposal, one complete copy, all of the sponsor's forms (if appropriate), and the Transmittal Form with the first three signatures is then brought to the Office of Grants and Contracts.

6. **OGC will obtain the last two signatures on the Transmittal Form and will secure the signature of the authorized institutional official on all other forms as required.** If you have questions about completing any item on this form, please consult the OGC. A PROPOSAL FROM THE UNIVERSITY IS ONLY VALID WHEN SIGNED BY THE APPROVED AUTHORIZED OFFICIAL OF THE UNIVERSITY (Chancellor, Provost, Assistant Provost for Planning, Programming & Academic Budgeting, Vice Chancellor for Administrative and Fiscal Services, and the Director, Office of Grants and Contracts).
7. When the Internal Review and Transmittal Form and any other necessary forms have been signed, the Office of Grants and Contracts will provide copying services and will assume copying & mailing costs associated with the proposal. All proposals are sent out certified mail or express mail depending on the time available for meeting the deadline. Our express mail cut-off time is 12:00 noon.
Time and Attendance Reporting

Policy Overview

The University of Massachusetts at Dartmouth requires that all employees submit a record reflecting their hours worked and hours absent from work. All records will include time and attendance, vacation and sick leave accrual and use, and the reasons for all leaves of absence, whether paid or unpaid.

The Chancellor is ultimately accountable for maintaining accurate time records that support university policy. The Chancellor may delegate this responsibility to the heads of the various operating units, and they, in turn, may delegate this responsibility to the department heads. The head of each primary operating unit is responsible for verifying and assuring the unit’s compliance with policy.

Employees will be paid on a bi-weekly pay frequency. All media of time records, e.g., timesheets, requests for leave authorizations, must be maintained for seven years.

Procedure

Timekeeping functions are decentralized and take place within the various departments campus-wide. The schedule for submission of time records in the PeopleSoft Time and Labor timekeeping system is weekly. All time must be recorded by the specified deadline of the pay period.

All employees and supervisors should carefully complete and review timesheets as submission by the employee and the supervisor’s approval certifies that the time reported correctly reflects all time worked and absences for the pay period indicated.

Authorization for overtime hours and compensatory time must be documented on the employee timesheet using specific time reporting codes and an explanation or justification for the authorization.

All employee timesheets require certification by an authorized department head signatory as follows:

This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.
Policy:

Responsibilities for supervision and timekeeping functions are segregated from personnel, payroll processing, disbursement, and general ledger functions.

Procedures:

1. Supervision and timekeeping functions are decentralized and take place within the various departments campus-wide. All other personnel and payroll related functions are managed within the Human Resources office.
Policies and Procedures
Payroll

Policy:

Records and controls exist for timekeeping and attendance.

Procedures:

1. The University utilizes the PeopleSoft Time and Labor timekeeping system to record time and attendance for all employees.

2. The University has developed a PeopleSoft End-User Training Participant Guide (the “Guide”) for time and attendance reporting. The Guide establishes best practices for managing time collection and is used throughout the University system.

3. All employees responsible for managing time collection receive a copy of the Guide. Classes are held as needed by the Human Resources office to train employees responsible for managing time collection within their respective departments.

4. Employee time and pay-related information is recorded on an Employee Timesheet. Timesheets are provided in the Guide for the various types of payroll, e.g., exception reporting, positive reporting, overtime, correction. Customized templates have been prepared and can be accessed electronically through administrative computing.

5. Timesheets are prepared weekly and entered by the Timekeeper into PeopleSoft. All time must be recorded by the specified deadline of the pay period.

6. The Timekeeper reviews the timesheets for accuracy and completeness in preparation for entry. If information is inaccurate or missing, the Timekeeper will follow up with the employee or the employee’s supervisor to complete the necessary data collection.

7. The Timekeeper reviews the error message report (TL007) after the nightly batch processing and the Edit Time and Apply Rules processes have been executed. This report will display any errors that have occurred and that need to be corrected prior to pay period processing.

8. All timesheets require the signature of the employee’s supervisor.

9. Timesheets are maintained by the respective department as an original source document for a period of seven years as prescribed by university policy.
Policy:

Hours worked, overtime hours, and compensatory time are authorized and approved by the employee’s supervisor.

Procedures:

1. Hours worked for positive reporting employees, overtime hours, and compensatory time are authorized, reviewed, and approved by the Department Head or his/her designee.

2. Hours worked, overtime hours, and compensatory time are reported on the Employee Timesheet and require the signature of the Department Head or his/her designee.

3. Authorization for overtime hours and compensatory time is documented on the Employee Timesheet using specific time reporting codes and an explanation or justification for the authorization.

4. All Employee Timesheets require certification by an authorized department head signatory as follows:

   This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.
Policy:

Appropriate payroll records are maintained for accumulated employee benefits, i.e., sick leave, vacation, personal time.

Procedures:

1. The PeopleSoft Time and Labor module, through use of workgroups, workgroup rules, and time reporting codes, accumulates leave accruals for all benefited employees.

2. Available time for individual employees to last pay date is displayed in the Leave Accruals panel. Leave accruals are “layered” in order by sick, vacation, and personal time.

3. Leave accrual verification is performed in conjunction with payroll processing utilizing the leave accrual verification report (UMTL 703) and reviewing for negative accruals.

4. Accrued liability reports for compensated absences for financial statement reporting purposes are prepared by the University Controller’s Office and University Business Systems.
Policy:

Procedures exist for authorizing, approving, and recording vacations, holidays, sick leave, and personal time.

Procedures:

1. Leaves of absence, to include vacations, holidays, sick leave, and personal time are reported and maintained on the PeopleSoft Time and Labor timekeeping system.

2. Leaves of absence are recorded on the Employee Timesheet and follow the same procedures as documented on records and controls for timekeeping and attendance.

3. Authorization and approval of leaves of absence are documented on the Employee Timesheet and follow the same procedures as outlined for hours worked, overtime hours, and compensatory time.
# Weekly Time & Attendance Report – Exception Reporting Employees

Department: ____________________________  Department ID: ____________________________  Week Ending (Saturday): ____________________________

<table>
<thead>
<tr>
<th>Employee ID</th>
<th>Empl Rec #</th>
<th>Name (Last, First, MI)</th>
<th>Shift</th>
<th>HR Account Code</th>
<th>Time Reporting Code</th>
<th>*Sun</th>
<th>*Mon</th>
<th>*Tues</th>
<th>*Wed</th>
<th>*Thurs</th>
<th>*Fri</th>
<th>*Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Report hours in decimals

This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.

Signature of Department Head: ____________________________  Date: ____________________________
Overtime Report – Exception Reporting Employees

Department: ___________________________  Department ID: ___________________________  Week Ending (Saturday): ___________________________

(Month/Day/Year)

<table>
<thead>
<tr>
<th>Employee ID</th>
<th>Empl Rec #</th>
<th>Name (Last, First, MI)</th>
<th>Shift</th>
<th>HR Account Code</th>
<th>Time Reporting Code</th>
<th>*Sun</th>
<th>*Mon</th>
<th>*Tues</th>
<th>*Wed</th>
<th>*Thurs</th>
<th>*Fri</th>
<th>*Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Report hours in decimals

Reason for Overtime

This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.

TL002 __ Weekly Time & Attendance Report Exception Hourly Employees

Signature of Department ___________________________ Date ___________________________

Internal Control Plan 82 August 31, 2005
Correction Form

Weekly Time & Attendance – Exception Reporting Employees

Employee Name: ____________________________________________  (Last, First, MI)  
Employee ID: ______________________________  Empl Rec #: ____________________________
Department: ______________________________  Department ID: __________________________

☐ Correcting Previously Reported Time  ☐ Time Never Submitted

The following data was incorrectly reported for the above named employee for week ending ____________________________ which is a previous pay week. Please correct and replace with the following:

<table>
<thead>
<tr>
<th>Account #</th>
<th>Time Reporting Code</th>
<th>*Sun</th>
<th>*Mon</th>
<th>*Tues</th>
<th>*Wed</th>
<th>*Thurs</th>
<th>*Fri</th>
<th>*Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Report hours in decimals

This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.

Signature of Department Head: ____________________________  Date Submitted: ________________

Comments / Central Use

Type of Adjustment: __________  Process Pay Period End Date: ________________
## Weekly Time & Attendance Report – Positive Reporting Employees

<table>
<thead>
<tr>
<th>Employee ID</th>
<th>Empl Rec #</th>
<th>Name (Last, First, MI)</th>
<th>Shift</th>
<th>HR Account Code</th>
<th>Time Reporting Code</th>
<th>*Sun</th>
<th>*Mon</th>
<th>*Tues</th>
<th>*Wed</th>
<th>*Thurs</th>
<th>*Fri</th>
<th>*Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Report hours in decimals

This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.

Signature of Department Head: ____________________________ Date: ____________________________
### Weekly Time & Attendance Report – Part Time Faculty and Teaching Assistants

Department: ___________________________  Department IID: ___________________________  Week Ending (Saturday): ___________________________

<table>
<thead>
<tr>
<th>Employee ID</th>
<th>Empl Rec #</th>
<th>Name (Last, First, MI)</th>
<th>Shift</th>
<th>HR Account Code</th>
<th>Time Reporting Code</th>
<th>*Sun</th>
<th>*Mon</th>
<th>*Tues</th>
<th>*Wed</th>
<th>*Thurs</th>
<th>*Fri</th>
<th>*Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Report hours in decimals

This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.

Signature of Department Head: ___________________________________________  Date: ___________________________
Contact Person: __________________________
Phone Number: __________________________
E-mail: __________________________

Positive Reporting – Late Pay Form

☐ Student    ☐ Non-student

Employee Name: __________________________ (Last, First, MI)
Employee ID: __________________________ Empl Rec #: __________________________
Department: __________________________ Department ID: __________________________
HR Account Code: __________________________ Hourly Rate: __________________________

<table>
<thead>
<tr>
<th>Time Reporting Code</th>
<th>*Sun</th>
<th>*Mon</th>
<th>*Tues</th>
<th>*Wed</th>
<th>*Thurs</th>
<th>*Fri</th>
<th>*Sat</th>
<th>*Total</th>
<th>Week Ending Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Report hours in decimals

This payroll has been processed in accordance with the University’s Payroll Expenditure Policy and the University’s Internal Control Plan. The amount listed has been certified to the Controller through the payroll system for payment. This certifies that time and attendance for each employee is on file in this department and has been authorized and approved by the appropriate manager to support amounts paid. This authorization and approval and supporting documentation will remain on file in this department for seven years for review by the University Auditor, campus internal auditing, or other auditing entity.

Employee Signature: __________________________ Date: __________________________
Supervisor Signature: __________________________ Date: __________________________
Policy:

Purchases of goods and services are initiated by properly authorized requisitions bearing the approval of officials designated to authorize requisitions.

Procedures:

1. The *University of Massachusetts Policy for Management of University Funds* describes procedures to establish and administer all funds as authorized by Section 11 of Chapter 75 of the Massachusetts General Laws, as amended.

2. The University makes use of a fully automated on-line purchasing system designated Enterprise Management and Performance Through Administrative Computing (*empac*). The *empac* project is a combined effort of all the campuses to implement the PeopleSoft Finance System.

3. The purchasing process begins with the requesting department initiating a Departmental Purchase Request (DPR) form. All such forms must be completed and signed by an authorized spending authority.

4. Requests are entered directly as purchase orders by the requesting department. The data entry operator (DEO) submits the purchase order for approval.

5. All approvals are performed electronically. There are several levels of approval depending on type of expenditures, source of funds, and dollar amount. See *On-Line Purchasing System Flow/Procedures* (appendix) that further details the approval process.
Policy:

Unobligated funds are verified by the accounting or budget department as sufficient to meet the proposed expenditure.

Procedures:

1. Budget Checking in the e*mpac Finance Application takes place through its Budget Checking Module (BCM), which is the component that enforces budgetary control on financial transactions.

2. The BCM verifies that all accounting transactions that originate in the application are tracked and controlled against their appropriate budgets. There are five budget types: Appropriation, Allotment, Organization, Revenue Estimate, and Project/Grant. Purchasing commonly uses the Organization budget, which is impacted every time the BCM processes a purchasing transaction.

3. All purchase orders entered into the e*mpac Finance Application Purchasing system must be posted before they are processed through the Journal Generator to create general ledger journal entries. Budget checking is a prerequisite to posting. All purchase orders are budget checked against the budget types in the system. After they pass budget checking, the encumbrances are posted to the controlled budgets ledger and the actuals ledger.

4. During budget checking the system verifies that the account type requires budgetary control, validates the transaction date against the detail calendar associated with the ledger, validates the transaction type to ensure it is valid, and verifies, on a transaction-by-transaction basis, that the total committed and/or expended amount does not exceed the budgeted amount. Any time a purchase order is created, an encumbrance is applied and the budget is impacted. When the transaction passes all of the above requirements, the BCM immediately updates the budget amounts in the budget ledger so that the expenditure and commitment totals for any ChartField combination are kept up to date. A new purchase order, or an increase to the amount of an existing purchase order, increases the encumbrance.

5. If budget checking fails, the BCM marks the transaction as an error and does not allow the transaction to be posted until the error is corrected. All budget checking errors can be evaluated and rectified through the Budget Checking Exceptions Panel.
UNIVERSITY OF MASSACHUSETTS
Dartmouth Campus

Policies and Procedures
Purchases and Accounts Payable

Policy:

Encumbrance entries are recorded only on the basis of approved purchase orders.

Procedures:

1. All purchase orders entered into the e*mpac Finance Application Purchasing system must be edit checked, budget checked, and approved before dispatched to a vendor. Once approved, an encumbrance is applied and the budget is impacted.

2. The Budget Checking Module immediately updates the budget amounts in the budget ledger so that the expenditure and commitment totals for any ChartField combination are kept up to date.

3. A new purchase order, or an increase to the amount of an existing purchase order, increases the encumbrance.
Policy:

Competitive bidding procedures are used.

Procedures:

1. Any purchase requisition for competitive products/services in excess of $5,000 not covered by a State or Massachusetts Higher Education Consortium (MHEC) contract, or that exceeds the dollar limit published for the respective University contract, shall be competitively bid.

2. Policies and procedures for competitive bid requirements are detailed in the *University of Massachusetts System Purchasing Manual.*
UNIVERSITY OF MASSACHUSETTS
Dartmouth Campus

Policies and Procedures
Purchases and Accounts Payable

Policy:

Purchase orders and contracts are issued under numerical or other suitable control.

Procedures:

1. Purchase order numbers are automatically generated by the e*mpac Finance Application upon saving a purchase order.

2. Each purchase order number is a 10-character value that is uniquely numbered for each campus. The first four (or in some cases, five) numbers indicate which campus business unit the purchase order is from, and the last numbers indicate the purchase order itself. For example, a purchase order from Dartmouth will have the prefix 0003, followed by the purchase order number (for instance, 00064), which will appear as 0003000064.
Policy:

Changes to purchase orders and contracts are subjected to the same controls and approvals as the original agreement.

Procedures:

1. Change orders are created manually or automatically when a dispatched purchase order requires modifications that affect the vendor's shipment to the University.
2. A change order may be created for any quantity not yet received or vouchered
3. Change numbers occur in numerical sequence so that changes to purchase orders can be tracked. The change number is maintained for the header, each line, and each schedule on a dispatched purchase order.
4. Change orders are generally created by the departmental data entry operator.
5. Changes that affect the budget charged, e.g., increase or decrease in the amount charged or changes to the chartfield string will initiate the approval and budget checking process.
6. See *On-Line Purchasing System Flow/Procedures* (appendix) that further details the change order process.
Policy:

Procedures exist to verify that goods and services have been received, quantities and prices are as ordered, and the goods and services meet quality standards.

Procedures:

1. The receiving process involves recording the items delivered and comparing the shipment to what was originally ordered through a purchase order.

2. The e*mpac Finance Application allows for the creation of an electronic receipt that includes delivery of multiple purchase order line items or many receipts that each include a partial delivery of line items from one purchase order.

3. Receiving is required for line item specific orders for goods with a total purchase order value of $1,000 or greater.

4. Valid vendor invoices are data entered as purchase order vouchers.

5. The e*mpac Finance Application makes use of an automated matching process that compares voucher information to the purchase order and receipt information (3-Way Match). A voucher must reflect the amounts and prices indicated on the purchase order before payment can be generated. Furthermore, receiving documents must likewise verify that the proper quantities have been delivered and are in acceptable condition.

6. Vendors are identified in the master vendor file to default to a 3-Way Match Rule in anticipation of goods received. Services (2-Way Match) and blanket purchase orders do not require electronic receipts.

7. If the information regarding price, quantity, and account distribution match the information entered as a voucher, payment can be made to the vendor, provided that the voucher passes budget checking and is approved.

8. Campus distribution services, the receiving management system, and payment for goods and services are detailed in On-Line Purchasing System Flow/Procedures (appendix).
Policy:

Procedures exist to record and follow up on partial deliveries.

Procedures:

1. An assigned individual within the Requesting Department is responsible for checking shipments for accuracy and hidden damage.

2. A Delivery/Acceptance Sheet/Packing Slip is submitted by Campus Distribution Services to the Departmental Receiver, who signs onto the Purchasing System and records receipt of the materials.

3. If the Department elects to reject all or part of the shipment, the Departmental Receiver will enter the receipt and indicate the reason for rejection on the Receiver Schedule Details sub panel. Only those items that are marked as being Accepted can/will be paid.

4. If the Department elects to withhold payment on a purchase order that does not require an electronic receipt, i.e., purchase orders under $1,000, services, or blanket purchase orders, the Department will notify Accounts Payable.

5. Campus distribution services, the receiving management system, and payment for goods and services are detailed in *On-Line Purchasing System Flow/Procedures* (appendix).
Policy:

The accounting and purchasing department are promptly notified of returned purchases, and such purchases are correlated with vendor credit advices.

Procedures:

1. If the Department elects to reject all or part of the shipment, the Departmental Receiver will enter the receipt and indicate the reason for rejection on the Receiver Schedule Details sub panel. Only those items that are marked as being Accepted can/will be paid.

2. If the Department elects to withhold payment on a purchase order that does not require an electronic receipt, i.e., purchase orders under $1,000, services, or blanket purchase orders, the Department will notify Accounts Payable.

3. Campus distribution services, the receiving management system, and payment for goods and services are detailed in On-Line Purchasing System Flow/Procedures (appendix).
Policy:

Controls exist for submission and approval of reimbursements to employees for travel and other expenses.

Procedures:

1. The University currently has in place an Employee Travel Policy and Business Expense Policy to ensure compliance with applicable state and federal laws and to establish guidelines for the approval, control and accounting for employee and Trustee travel on University business (see Policy for Management of University Funds: Appendix B and Appendix C).
Policy:

Controls exist for processing invoices not involving materials or supplies, e.g., lease or rental payments and utility bills.

Procedures:

1. Lease or rental payments and utility bills are subject to the same controls as payment for goods and services.
2. Encumbrance entries are recorded only on the basis of approved purchase orders.
3. Funds for lease or rental payments are generally encumbered for the lesser of remaining payments under the lease or rental contract or through the end of the fiscal year.
4. Funds for utility bills are estimated and encumbered for the fiscal year through the use of a blanket purchase order.
5. Lease or rental payments and utility bills are subject to the 2 – Way Match Rule, as they do not require electronic receipts.
Access to the master vendor file is limited to employees authorized to make changes.

1. The Purchasing Department is the custodian of the master vendor file.
2. The Accounts Payable Department has the ability to update remit addresses only.
Responsibilities for the requisitioning and receiving functions are segregated from the purchasing, invoice processing, accounts payable, and general ledger functions.

1. The University is departmentalized in all functions relating to the purchasing, receiving, and payment of goods and services to avoid the possibility of employees performing incompatible functions. See Organization Chart appended to the Internal Control Plan.
Policy:

An accounts receivable event is established whenever goods or services have been provided and corresponding earnings are measurable.

Procedures:

1. Assessment of charges for new and continuing students is managed through the Student Information System (SIS), an automated software system.

2. The Bursar is responsible for creating the rate table used by SIS in assessing charges. The rate table is based on approved charges for tuition and fees established by the Board of Trustees. This procedure is performed prior to generation of the billing statements and is usually done in early July for the fall semester and mid-November for the spring semester.

3. The Systems Analyst based on a schedule prepared by the Bursar performs batch process tuition and fee calculations. Tuition and fee calculations for the fall semester begin the first week of July and continue on a weekly basis until two weeks prior to the due date. The due date for the fall semester is typically the Friday of the second full week in August. For the spring semester the schedule remains the same as for the fall semester with the first tuition and fee calculation occurring the last week in November and the due date is the first Friday in January.

4. On-line tuition and fee assessment may be performed to assess charges on a student’s account at anytime after the rate table has been established.

5. Tuition and fee assessment procedures are documented in the SIS Billing/Receivable Manual and also in the SIS On-Line Reference System.
Policy:

The responsibility of billing revenues is segregated from collections and general ledger posting.

Procedures:

1. The Bursar is responsible for assessing charges and preparing statements for mailing.
2. The University Enrollment Center is responsible for collections including processing mail and credit card payments.
3. General ledger postings relating to revenues and collections are generally accomplished through automated feeds generated by the Billing and Receivables System (BRS).
Policy:

Procedures exist for the timely billing of amounts due.

Procedures:

1. Student Billing Procedures
   a. The Systems Analyst based on a schedule prepared by the Bursar performs batch process billing using the population selected in performing tuition and fee calculations.
   b. The generation of billing statements follows the same schedule as assessment of charges. Billings for the fall semester begin the first week of July and continue on a weekly basis until two weeks prior to the due date. The due date for the fall semester is typically the Friday of the second full week in August. For the spring semester the schedule remains the same as for the fall semester with the first billing occurring the last week in November and the due date is the first Friday in January.
   c. Subsequent billings prior to the applicable semester due date will include all charges assessed since the previous billing.
   d. Billing procedures are documented in the SIS Billing/Receivable Manual and also in the SIS On-Line Reference System.

2. Third Party Billing Procedures
   a. Students submit documentation from the agency responsible for payment or partial payment of their student account to the Bursar’s Office.
   b. The University does not accept third party agencies that will pay based on the final grade.
   c. An invoice is prepared in the Bursar’s Office for the applicable students along with any other documentation required by the agency.
   d. Third party agencies currently include:
      - Massachusetts Rehabilitation Commission
      - Massachusetts Commission for the Blind
      - Corporation for Business, Work, and Learning
      - Department of the Navy
      - Embassy of the State of Kuwait
      - Veteran Rehabilitation and Counseling
      - Americorp
      - Miscellaneous Businesses
   e. Invoices are prepared after the add/drop period for each semester. This period is typically the first 5 days of each semester.
Policy:

Balances of individual receivable accounts are periodically reconciled with general ledger control accounts.

Procedures:

1. The Bursar will periodically reconcile the individual receivable accounts to the general ledger control accounts.
2. Receivables are reconciled using the BRS Audit, which is a Focus-generated report that summarizes transactions by subcode.
3. BRS Audit is reconciled to the general ledger control accounts using a PeopleSoft finance report, UMGL 7046, Balance Sheet.
Policy:
Delinquent accounts are reviewed and considered for collection procedures on a timely basis.

Procedures:
1. The Bursar reviews delinquent accounts for collection procedures on a periodic basis.
2. The University adheres to the Commonwealth’s debt collection policies (see Comptroller Policy Memo # 318).
3. Accounts will remain in collection until all efforts have been exhausted by the debt collection agency at which time they will be presented for write-off.
Write-offs and other reductions of receivables and refunds of amounts previously collected follow prescribed policies and procedures.

1. Write-offs
   a. The University adheres to the Commonwealth’s debt collection policies (see Comptroller Policy Memo # 318).
   b. Accounts will remain in collection until all efforts have been exhausted by the debt collection agency at which time they will be presented for write-off.
   c. The Bursar’s Office will prepare a worksheet listing names, student ID, amounts and types of charges to be written off.
   d. The State Comptroller’s Office approves tuition write-offs.
   e. Student fees, including housing and board, are approved by the campus controller for write-off.
   f. The Bursar’s Office maintains detail for each charge written off and places a hold on the student account to prevent future registration and release of transcripts.

2. Tuition Waivers
   a. The University has established policy on tuition waivers documented and detailed in Trustee Document T96-129. The Policy governs all waivers of tuition including waivers provided pursuant to Section 19 of Chapter 15A of the General Laws as well as waivers of tuition for University employees.
   b. Tuition waiver policy is further documented in the Board of Higher Education (BHE) Tuition Waiver Program Guidelines.

3. Student Refunds
   a. The student refund policy is approved by the Chancellor and documented in the University catalog.
   b. The refund percentages are entered into the Student Information System (SIS) on the refund tables included in the rate table. The Bursar maintains these tables.
   c. The Registrar’s Office notifies the Bursar’s Office when a student withdraws from the University. Executing an on-line tuition calculation (screen 407) recalculates the student’s account.
   d. If a balance exists, a bill is sent to the student. A hold flag is placed on the account to prevent any future registrations or release of transcripts until the outstanding balance is paid.
3. Student Refunds (Continued)

e. If a credit balance exists, depending on the method of payment, a check or credit card refund is generated. If payment was made by check, there is a 30 day wait period from the date the payment was made before issuing a refund check to allow the check to clear the bank.

f. Refunds are processed in the Bursar’s Office on SIS by using refund-specific subcodes. Transactions using the refund specific subcodes are fed to Accounts Payable.

g. Student refund procedures are documented in the SIS Billing/Receivable Manual and also in the SIS On-Line Reference System.
Policy:

Tuition and fee waivers, bad debt write-offs and other allowances are approved independently of processing, recording, and collecting the charge.

Procedures:

1. Tuition and fee waivers are approved either by external agencies or other departments within the University depending upon the type of waiver. Proof of tuition waived is presented to the University Enrollment Center, which is responsible for processing and recording the waiver.

2. Bad debt write-offs follow prescribed policies and procedures. The State Comptroller’s Office approves tuition write-offs. Student fees, including housing and board, are approved by the campus controller for write-off.
University of Massachusetts
Responsible/Acceptable Use of Computing and Data Resources

University data, 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 are protected from misuse and that both the computer systems and the data stored in them be accessed and maintained in a secure environment.

This document outlines the standards for the acceptable use of University data (regardless of the medium on which it resides and regardless of its form), and computing systems/resources which include, but are not limited to: hardware, software and communications equipment (e.g. voice and data networks, servers, routers, modems, etc.) used in the processing, transmission and storage of electronic data. This document does not waive any claim that the University may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through University computing systems.

These standards comply with and are based on the laws of the Commonwealth of Massachusetts and the United States and other regulatory agencies. Other University Standards/Guidelines (Data Security & Classification, Electronic Communications, World Wide Web, Wireless Technology, etc.) and/or campus procedures may impose certain restrictions that are not specifically covered by state and federal law, or other regulations.

Definitions related to this document can be found in the Data and Computing Guideline Definitions.

These standards apply to all:

a. Computer systems owned, leased or maintained by the University. This includes:
   mainframe, mini and microcomputers/PCs; servers; networks (regardless of type - LAN,
   WAN, wireless, etc.); routers; bridges; hubs; and various peripheral equipment
   including
   but not limited to printers and modems.

b. Authorized Users - all students; 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, University
   computer systems/networks or software applications (e.g., email, Internet,
   registration, etc.) to perform their job function, academic assignment, or contractual
   obligations.

   c. University data regardless of the medium on which it resides (e.g., tape, cartridge, disk, hard drive, etc.), and regardless of its form (e.g. text, graphic, video, voice, etc.).
d. Electronic mail (e-mail) created within, sent to, maintained within, or administered by the electronic mail systems of the University of Massachusetts.

GENERAL

Since many users share information data and technology, and because of legal and ethical requirements, all students and staff need to be aware of their responsibilities related to data and computing at the University of Massachusetts. Remember that observing these standards will help to make computing and use of the network services more pleasant for all. Please use the University data and computing FAQ (http://security.umassp.edu/?fuseaction=faqs.index) to clarify policy, standard/guideline, and use questions.

Access may be given to: manual data processing systems, 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 worldwide networks such as the Internet. Information resulting from communication on University computer systems is University property. Authorized users are presumed to be responsible for any activity carried out under their University Logon Ids/Operator Ids/Accounts. Employees who access University or Campus networks for private purposes should subscribe to a commercial service provider.

Every employee and student at the University is responsible for implementing security in their daily interactions with people, data, systems, and facilities. As they perform their normal functions they should be alert and conscious of the security environment around them and notify the appropriate security/system administrators when they notice a security vulnerability, system/software malfunction, possible security incident (e.g., virus, system compromise/hacking), or if they have suggestions for improvement.

University employees, students and all users accessing University data or computing systems/resources shall exercise responsible, ethical behavior when using University data and computing systems/resources including, but not limited to:

- Adhering to all laws governing data security and use including Copyright Laws, Electronic Communications Privacy Act (ECPA), Digital Millennium Copyright Act (DMCA), Health Insurance portability and Accountability Act of 1996 (HIPAA), Computer Fraud and Abuse Act (CFAA), TEACH Act, etc.

- Complying with University acceptable use and other policies/standards and guidelines when accessing any University data, computer systems/resources, networks. By accessing any University data or by using any University computing system/resource, University employees, students and users agree to comply with this and all University data and computing related policies/standards/guidelines (e.g., Data Security and Classification, Wireless Technology, World Wide Web, etc.). Full text of University data and computing policies/standards/guidelines are located at http://www.umassp.edu/policy/#data.

- Complying with University acceptable use and other policies/standards and guidelines when accessing any other networks or sites from University computing systems/resources. The University and/or Campus networks may enable authorized users to connect to computers at other educational and research institutions, and connect to many computers in organizations not related to the
educational sector. The fact that you can connect to a computer system does NOT automatically give you authority to use that computer system. The mere lack of security on a network does not mean that a computer system is open and available for use by unauthorized users. 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. Additionally, any network traffic exiting the University system is subject to the acceptable use policy/standards/guidelines of the network through which it flows. 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.).

- Only accessing University data and/or computer systems/resources for which they have been authorized. Access to data is given to authorized users. This access should not be shared, transferred or delegated (e.g., authorized users should not access data and then let others use that data). Access to data classified as Private, Restricted or Confidential is based on legal requirements or on a need to know; job function; or course requirement basis. Many computers in the University are connected to the University and/or Campus networks. Individuals must have an authorized logon id/operator id/account to access any University computer system including networks.

- Using their access to University data and computing systems/resources for approved purposes only. Approved purposes include work related to student studies or instruction, the performance of duties by an employee, or other University sanctioned activities. Access to data, assignment of Logon Ids/Operator Ids/Accounts and deployed network connections are made available to benefit the entire University and support its missions of education, research and public service including instruction, research, administrative tasks and collaborative activities with other entities, including but not limited to colleges/universities and private businesses. The University does allow for employees' personal pages that provide information about an individual that is relevant to that individual's role at the University.

- Safeguarding the integrity, accuracy and confidentiality of University data by taking reasonable efforts to protect University data and computer systems/resources from theft; destruction; unauthorized creation, alteration or exposure (e.g., unauthorized updating, processing, outputting, or distribution); or any form of compromise resulting from inappropriate intentional, negligent acts, or omissions. This includes implementing appropriate physical security and data classification procedures, and periodically "refreshing" downloaded data to ensure you are working with accurate, up-to-date data.

- Properly creating, accessing, using and disposing of University data based on the data's classification (See Data Security & Classification Guidelines). Users shall access University data for approved purposes only, and shall understand the data they are accessing and the level of protection required. 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.
• Implementing appropriate levels of security on all manual and computer systems/resources on which Private, Restricted, Confidential (As defined in the University Data Security and Classification Guidelines) or critical data is stored, maintained, or in the case of electronic systems, transmitted.

• Appropriately backing up data (e.g., business, personal/instructional, etc.), and computer system and applications software to allow for recovery if there is a disruption. Multiple generations of operating system, application and data backups should be maintained in both on-site and off-site storage facilities.

• Ensuring that antivirus software is installed and continuously enabled on any computer system they use which accesses University data or computing systems/resources. This will ensure the spread of viruses within the University networks and computer systems is prevented.

• Scanning software downloaded from an email, network or installed from a disk/CD-ROM for possible virus infection before you use it.

• Properly using shareware and public domain software. 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.

• Using all non-software proprietary information (e.g., text, images, icons, programs, etc.) retrieved from computer or network resources in conformance with laws.

• Addressing issues of incompatibility to previous versions, etc. of all supported software running on the affected computer system when performing software upgrades.

• Using standard systems development life cycles and include system testing and documentation when developing on a microcomputer/PC, critical or impacting applications (As defined in the University of Massachusetts Business Continuity Guidelines) or applications used to process administrative data.

• Contacting the appropriate system, network and/or security administrators(s) prior to performing any academic game development, computer security research, or the investigation of self-replicating code as part of an academic or instructional activity. This will allow the administrator to determine and evaluate possible effects on the system being used for these activities.

• Following the same standards of intellectual honesty and plagiarism in regards 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.

• Notifying the appropriate system, network and/or security administrator(s) of any suspected or actual security violations/incidents.

• Being aware that the University disclaims any loss or damage to software or data that results from its efforts to enforce this and other data and computing Guidelines.
University students and employees shall:

- Attend a data security orientation,
- Sign a computing the University Computing Awareness and Data Security Compliance Statement and
- Reaffirm annually that they know and understand University policies/standards/guidelines and Campus procedures regarding data and computer use.

**ELECTRONIC COMMUNICATIONS**

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 communications 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 communication users need to be aware of the vulnerabilities in electronic mail communication and of the legal responsibilities that accompany the use of this medium.

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 employees' job function.

The University considers a personal e-mail message to be private correspondence within the limits set forth in this and other applicable standards/guidelines and policies, however, the University has the right to look at any documents/files including emails stored, sent or received on/across University computer systems and networks if necessary for University business.

Due to information technology, the privacy, security and authorship/source of documents and messages stored in and transmitted via electronic media cannot be guaranteed. Users of electronic communications are cautioned that such messages might become available to others. Emails can be stored, copied, printed or forwarded by recipients. As such, email users should not write anything in an email that they would not feel just as comfortable putting in a memo.

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.

University E-mail Users shall use e-mail in a responsible manner consistent with other business communications (e.g., phone, correspondence) including, but not limited to:

- Safeguarding the integrity and confidentiality of University electronic mail.
- Only using mail IDs assigned to them.
• Removing mail from their mailbox consistent with University, campus, departmental or electronic mail administrator message retention procedures and these Guidelines.

SECURITY
Be particularly careful of your password. Do not give/share your password to/with anyone or type your password when someone is watching. This includes logging on for another person and allowing them to access computer systems under your logon/operator id. Do not write down your password or store it in batch files, automatic login scripts, terminal function keys, or in other locations where another person might discover them. Do not hard-code passwords or pin numbers used to protect access to University data in software or scripts. Once someone has your password it is possible both to look in your directory and to use your username for malicious purposes.

Follow password security standards including, but not limited to selecting a password that is difficult to guess and when possible, includes letters, digits and special characters (e.g., #, %,$). Logon/Operator Ids, names, birth date, employee or 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. You should also avoid using any personally identifiable information (e.g., pet’s, child’s or spouse’s/partner’s name; favorite sports team or car; etc.).

Log off computer systems/resources if you leave your pc unattended or will not be accessing data for an extended time. Staying logged on leaves your id and the system vulnerable for misuse. You are responsible for all activities that take place from your account.

Although the University makes a reasonable effort to protect files stored on the university systems from being accessed by anyone other than authorized individuals, the University cannot guarantee the confidentiality of any of these files. Programs and files are considered confidential unless they have explicitly been made available to authorized users.

Possible loopholes in computer or network system security shall 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.

PRIVACY
University computer systems/resources may record information about each user session. Information recorded includes the username/operator id associated with the session, the login and logout dates and times, and the amount and kind of computer resources used during the session. This information is used for legitimate University purposes including issues of law, abuse, security or system managements.

The University does not routinely monitor the content of computer systems/resources including files, programs and electronic communications/emails. The University has the responsibility and authority to access, review and release University data, electronic information that is transmitted over or stored in University systems or facilities, and to monitor individual accounts to the extent the University determines to be reasonably necessary for legitimate administrative purposes, including but not limited to a determination by appropriate University officials that there is a reasonable basis to believe that such action:

1. Is necessary to comply with legal requirements or process, including but not limited to subpoenas, writs or warrants;
2. May yield information of use in the investigation of a suspected violation of law or of University policies, procedures and codes of conduct; or when a system security or system operation has been compromised or used for unauthorized activities;
3. Is needed to maintain or protect the integrity or operations of University computing systems;
4. May yield information needed to deal with an emergency; or
5. In the case of University employees and officials, may yield information that is needed for the ordinary business of the University.

Additionally, the University has the responsibility and authority to scan computers attached to the University’s wired and wireless networks to ensure appropriate security, and support network operations and performance.

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, network or 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 system, network or 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.

The University will take reasonable steps to protect the rights to privacy granted by the Federal Family Educational Rights and Privacy Act of 1974, as amended, 20 U.S...C. Sec. 1232g, the Electronic Communications Privacy Act of 1986, Pub. L. 99-508, the Massachusetts Fair Information Practices Act, M.G.O. c. 66A, and other applicable laws. The content of some electronic communications may be deemed public records under the Massachusetts Public Records Act, M.G.L. c. 66.

Remember that any printouts in public places are likely to be seen by others.

WORKSTATIONS AND MICROCOMPUTER/PERSONAL COMPUTERS (PC)
Although micro-computing offers improved productivity and cost-effectiveness, it requires the implementation of additional controls in those areas in which Private, Restricted, Confidential (As defined in the University Data Security and Classification Guidelines) or critical University data or hardware/software may be at risk. University employees, students and computer system/resources users shall exercise appropriate pc security including, but not limited to:

- Microcomputer/PC keys shall not be left in the computer when unattended. These keys shall be properly secured.
- All workstations and microcomputer/PC systems shall be outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressers, as appropriate.
- If environmental conditions pose a significant risk of static electricity discharge, all potentially effected workstations and microcomputers/PCs shall be outfitted with static protection equipment. This ensures that the discharge of static electricity does not damage computer equipment or data.
• Appropriate hardware and software security (e.g., cable lock downs; password access control; data compression and encryption; audit log of access, updates; etc.) shall be placed on all microcomputers/PCs and transportable computers that have Private, Restricted or Confidential data (As defined in the University Data Security and Classification Guidelines) stored in them (i.e., on the local drive).

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

• Whenever a hard disk is sent for repair, the vendor shall be required to comply with University Data Security and Classification Guidelines regarding the handling of data.

• When disposing (e.g., recycling, salvaging, transferring ownership to another party, etc.) of microcomputer/PC hard disks, the hard disks should, at a minimum, be low level formatted so as to erase all data on the hard drive.

• Staff and students loaned or using University owned/funded transportable computers shall make every reasonable effort to secure and safeguard the physical integrity of the computer and to comply with all Data Security and Classification Guidelines.

• Security tokens shall not be stored with the microcomputers/PC’s (including transportable computers).

• Passwords, University assigned pin numbers (excluding telephone pin numbers) or logon /operator ids shall not be programmed in any computer accessing University networks or Private, Restricted or Confidential data (As defined in the University Data Security and Classification Guidelines). This includes transportable computers. Additionally, microcomputers/PCs shall not be configured to allow a third party to access any University network or data without being prompted and required to enter a password.

• All Private, Restricted and Confidential data (As defined in the University Data Security and Classification Guidelines) stored on workstations or microcomputers/PCs and not backed up centrally on a network, shall be backed-up on separate storage media after changes to the data have occurred. As noted previously, backups should be stored in an off-site location when possible.

• Private, Restricted and Confidential data (As defined in the University Data Security and Classification Guidelines) which has been backed-up shall not be used for data restoration purposes unless another back-up copy of the same data exists. This will prevent the only current copy of Private, Restricted and Confidential data from being inadvertently damaged in the restoration process.

• Proper disk maintenance practices shall be followed (e.g., clearly label diskettes; back up data, application and operating system diskettes; store away from extreme cold/heat; protect from dust, excessive moisture or water; keep away from magnetic devices including radios, telephones, keys, wall magnets; etc.)
All devices connected to the University and/or Campus networks must conform to these Standards, Guidelines, Campus procedures, and specific network requirements. Devices which do not comply, or which disrupt other network clients may be disconnected at the discretion of the appropriate system, network or security administrator.

**DATA, COMPUTER SYSTEM / RESOURCE ABUSES**

You can expect to lose your computer account; be disconnected from the network; be denied or given limited (i.e., to allow for the performance of required academic or employment related tasks) access to University data, applications and/or computer systems; and/or be subject to reprimand, suspension, dismissal/termination, or other disciplinary action. Additionally, these individuals may be charged with criminal offenses (either by the University or third parties such as the Record Industry Association of America) or have civil action taken for computer abuses including, but not limited to:

- Providing false or misleading information to obtain access to University computing facilities or resources.

- Unauthorized access to University data, computer systems/resources, or another's computer or email account. This includes using computing systems/resources to access any other computer system (on or off-campus) without authorization. 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.

- Accessing or copying 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.

- Attempting to compromise or tamper with user passwords. This includes, but is not limited to cracking, decoding, copying password files, "sniffing" packets to search for passwords or otherwise attempting to discover passwords belonging to other individuals. This also includes taking advantage of another user's naiveté to gain access to computer systems/resources or data, or preventing someone from using their account by changing the password or by other tampering.

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

- Connecting dial-up modems to workstations or microcomputers/PCs that are simultaneously connected to a network.

- Remotely logging into (or otherwise using) any microcomputer/PC not designated explicitly for public logons over the University and/or Campus networks, even if the configuration of the computer permits remote access, unless you has been given explicit permission from appropriate authorized personnel.

- Disseminating any confidential information unless such dissemination is required by the individual's job at the University.

- Deleting or copying files from another person's computer or email account.
• Posting, sending or publicly displaying or printing unsolicited mail or materials that violate existing laws or University policies/codes of conduct. Such material includes, but is not limited to those that are of a fraudulent, obscene, offensive, defamatory, harassing, abusive, or threatening nature. 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.

• Repeated sending of unsolicited mail.

• "Rebroadcasting" information obtained from another individual that the individual reasonably expects to be confidential.

• Abusing the networks to which the University belongs.

• Using University computer systems/resources or networks for monetary gain, political purposes or illegal activities. This includes using University Internet resources to create web pages for personal business or financial gain, except as permitted by other University policies.

• Illegally using of copyrighted materials including print, audio, and video.

• Illegally soliciting or distributing copyrighted software within or outside the University through any mechanism (e.g., email, bulletin boards, disk, etc.), electronic or otherwise. Employees and students shall not copy copyrighted software 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 software. The University does not own this software. Employees and students are required to comply with software licenses and the U.S. Copyright Act.

• Using personally owned software on University computer systems/resources unless the software is properly licensed for such use and system administrator approval has been obtained.

• Adding, copying or removing software to/from University computer systems/resources in violation of the software license. This includes copying software from or to University computer systems/resources.

• Intentionally writing, producing, generating, copying, propagating or attempting 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.

• Modifying the configuration of the University or Campus computing infrastructure by adding or removing network links, computers, or peripherals (e.g., external disks, printers, modems, video systems, etc.); reconfiguring any control switches or parameters; upgrading processors, expanding memory, installing extras circuit boards, etc., except as authorized by the appropriate system or network administrator.

• Unnecessarily or inappropriately using limited computer systems/resources including but not limited to such inappropriate uses as sending chain emails, spamming, mail bombing, generating unnecessary excessive print, etc. Chain letters have been illegal if sent through the United States Postal Service (USPS) for many years.
• Attempting to develop or use any mechanism to alter or avoid charges levied by the University for computing resources.

• Performing or assisting in the performance of any act that will interfere with the normal operation of computer, terminals, peripherals, networks, etc. or in any activity that interferes with the rights of others (e.g., Using public, lab or departmental equipment for personal entertainment when other authorized users need access to perform University related tasks; intentionally damaging or misusing any University computer system/resource including terminals, microcomputers/PCs, networks, printers or other associated equipment; etc.)

Reports of abuse to your account can be made by contacting your system administrator. Please also note that your campus may have additional acceptable use requirements. Contact your system administrator for more information.
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.

Acceptable Use of Data and Computing Resources

Definitions Addendum for Computer Security and Usage Guidelines, Data Security and Classification Guidelines and Electronic Mail Guidelines
Data and Computing Guidelines/Standards Definitions

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

**Access Control** refers to the process of limiting access to computing systems and resources to authorized users, programs, processes, or other systems.

**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.

**Advertising** is offering space on a web page/publication to another party for the purpose of promoting goods and services offered by that party in exchange for money, goods, or services.

**Alt Tags** are HTML codes that describe graphical elements in a web page/publication so that they are viewable by non-graphical browsers.

**Alternate Facility or Alternate Operating Site** is a temporary facility in which business functions will be performed during a recovery effort.

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

**Antivirus software** is software that detects the existence of viruses, trojans and other malware threats on your computer system.

**Application Administrator** is the individual responsible for the functional operation of a data system (manual or electronic) including, but not limited to, business resumption and recovery.

**Application Software** is a program(s) written to perform a business process such as payroll.

**Application Program Interface (API)** is a formalized set of software calls and routines that can be referenced by an application program in order to access supporting network services.

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

**Archival Records** are records which have continuing administrative, research or historical value, or which document the University's organization, functions, policies, decisions, procedures, or operations. Examples include organization charts, memorandum, minutes, architectural drawings, graduate theses and senior honors theses, personal papers, etc.
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) or a log of network hardware/software changes would be maintained to monitor what configuration changes were made and by whom.

Authenticated Digital Signatures is the digital verification of the identity of a person or process. In a communication system, authentication verifies that messages really come from their stated source, like the signature on a (paper) letter.

Authentication Or User Authentication is the process by which the identity of an individual and their right to access specific categories of data are verified.

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.

Baseline Level of Connection Service Quality is determined by factors that can affect radio transmissions, such as distance from the wireless access point (i.e., WAP), number of users sharing the bandwidth, state of the environment from which the transmission is taking place, and the presence of other wireless client devices that can cause interference.

Binary attachments refer to any file format for digital data encoded as a sequence of bits but not consisting of a sequence of printable characters (text). The term is often used for executable machine code.

Bridge is a device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to "filter" packets, that is, to forward only certain traffic.

Browsers or Web Browsers are software programs that display Internet based information as defined by HTML.

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).

Business Continuity Planning is the process of identifying critical data systems and business functions, analyzing the risks of disruption to the data systems and business functions, determining the probability of a disruption occurring and then developing plans to enable those systems and functions to be resumed in the event of a disruption. The process includes testing and maintaining the business resumption plans to ensure they are effective.

Business Disruption is an occurrence that impacts a data system to the extent that the capability to perform normal and routine operations is impaired.
**Business Resumption Plan (BRP)** is a document that details the steps to be taken in the event of a business disruption for a specific data system(s).

**BRP Coordination Site** is a temporary location with communication equipment from which initial resumption efforts are coordinated.

**Button Bars** are used to place fixed links between a series of pages to bind them into a document. In complex Web sites button bars may also be used to provide links to submenus, tables of contents, or other organizational pages.

**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 Administrative Services** refers to the President's Office, Institute for Governmental Services, Treasurer's Office, University Audit, University Controller, and University Information Technology Services.

**Campus Information Security Officer /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, control, oversight/monitoring, and coordination. This job function may be assigned to one or more individuals on a campus, and is not necessarily an official job title.

**Chain E-mail** refers to several types of e-mail messages including virus hoaxes, good luck/bad luck messages, and fake fund raisers that are sent out to several users and those users are asked to send the message to several more e-mail users and so on. Chain E-mail unduly strains the computing system and its resources.

**Checklists** refer to lists containing brief questions which when properly answered will reveal possible weakness in a system.

**Classified Data** refers to University data that has been identified as Operational, Private, Restricted or Confidential. See the University Data Classification and Confidentiality Policy for more information.

**Client/Server Technology** refers to an environment in which a software package running on one computer (server) is accessed by another computer (client) and the data stored in and processing occurs on the server.
Cold Site is a facility that contains no computing-related equipment except for environmental support such as air conditioners, water conduits, raised floors, motor generators, power outlets, and a security system made ready for installing computer equipment. This site may be University owned or vendor operated.

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.

Convenience Records are copies of Official Records maintained by departments other than the Official Records Custodian. This includes records of all mediums and types.

Computer/Computing System(s) refers to the hardware, software and communications equipment (e.g. voice and data networks, servers, routers, modems, etc.) used in the processing and storage of electronic data.

Conference Chat is the ability to interactively communicate on-line in a real-time mode.

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

Context-Sensitive Help is on-line documentation giving details about a word or topic.

Controls are mechanisms implemented to limit exposure, such as backing up data, storing backups offsite, using surge protectors and uninterruptible power supplies, running virus checking software and security software packages, etc.

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.

Coverage is the geographical area where a baseline level of connection service quality is attainable. Coverage area is also expressed as “footprint”.

Critical System is a data system considered to be integral to the accomplishment of the University mission(s) and its business functions, and without which University operations would be curtailed or otherwise severely impeded.

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

Data Compression refers to reducing the amount of storage space required to store a given amount of data, or reducing the length of message required to transfer a given amount of information.

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.

**Data Integrity** refers to the completeness and accuracy of data.

**Data Or Information Security** refers to the development and implementation of a reasonable system of measures/controls/safeguards to protect data (regardless of the medium on which it resides (e.g., tape, cartridge, disk, hard drive, etc.) and computing resources from unauthorized access, theft, removal, misuse, disclosure, and/or corruption so that data and computing resource availability and integrity is preserved. These controls 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 business continuity planning); Hardware; Software (e.g., network, operating and application system software); Data; Communications/Network; Physical and Environmental; Legal (e.g., state, federal & regulatory).

**Data System** is any method (e.g., manual, electronic or a combination of both) used to process data (e.g., this could include using paper ledger books, computerized processing, etc.).

**Database** is a formally structured collection of data or set of data that is required for a specific purpose.

**Database Management System (DBMS)** refers to a software system that facilitates the creation and maintenance of a database or databases, and the execution of computer programs using the database or databases.

**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.

**Device** refers to any part of a computer other than the CPU or working memory (e.g., disks, keyboards, monitors, mice, printers, scanners, tape drives, microphones, speakers, cameras, etc.).

**Disposition** refers to how records are handled once the retention period has been meet. Disposition includes archiving, transfer to another agency, or destruction.
**Disruption** is any situation or event which interrupts the routine and regular processing of data, thereby causing inaccessibility, harm or damage, sudden or serious misfortune or calamity, or the inability to perform these routine functions in part or in whole.

**Distributed Platform** refers to the fact the processing of data can be performed on various computers (e.g., mainframe, minicomputers, PC's, etc.) at different locations.

**Domain Name** consists of a sequence of names or labels separated by periods usually used to name Internet host computers uniquely.

**Dynamic Host Configuration Protocol (DHCP)** refers to a protocol that provides a means to dynamically allocate IP address to computers on local area networks. The network administrator assigns a range of IP addresses to DHCP and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server.

**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 that 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.

**Encryption** refers to the process of converting plain text into unintelligible forms (i.e., scrambling) in order to prevent any but the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security. Common types include Data Encryption Standard (DES) and RSA.

**Environmental Controls** refer to the simultaneous controlling of the characteristics of air, such as temperature, humidity, cleanliness, motion, and pollutant concentration, in a space to meet the requirements of the equipment.

**Executable Programs** refer to programs in machine language, which are ready to be run (i.e., the
process of carrying out the instructions in a computer program by a computer).

**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.

**Financial Records** are records related to billing, financial aid disbursements, insurance, purchasing, accounting, and other operationally oriented business functions.

**Finger Command** refers to a command that provides information about users on a network.

**Firewall** is a dedicated computer or device with special security precautions on it, used to filter outside network, especially Internet, connections and dial-in lines.

"**Flashable**" firmware is re-programmable software (programs or data) that has been written onto read-only memory (i.e., ROM).

**Full-Interruption Testing** describes a test in which the total business resumption plan for a data system(s) is activated. This test is costly, could disrupt normal operations and should be used and scheduled with extreme caution.

**Graphics Interchange Format Standards (GIFS)** are binary attachments that follow standards for digitized images.

**Graphical user interface (GUI)** is the use of pictures rather than just words to represent the input and output of a program. A program with a GUI runs under some windowing system (e.g. Microsoft Windows, etc.). The program displays certain icons, buttons, dialogue boxes etc. in its windows on the screen and the user controls it mainly by moving a pointer on the screen (typically controlled by a mouse) and selecting certain objects by pressing buttons on the mouse while the pointer is pointing at them.

**Homepage** refers to primary web page of an entity (e.g., University, department, person, etc.).

**Hopping Sequence** refers to the way a packet of data traverses between its source and destination.

**Hot Site** is a fully equipped data processing facility maintained on a standby basis for use in a business resumption operation.

**Hub** refers to a device within a network that accepts a signal from one point and redistributes it to one or more points.

**Human Resources Records** are non-payroll records related to University employees such as performance reviews, disciplinary actions, contracts, etc.
HyperText Markup Language (HTML) is code used to create Web pages/publications. These codes tell web browsers how to display the text (e.g., titles, headings, lists, etc.), link to other documents, and control character formatting (e.g., bold, italic, etc.).

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 (e.g., 15 minutes).

IETF conventions refers basic web development and security principles set up by the Internet Engineering Task Force (IETF) which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Image Map is a graphical navigational tool that allows parts of an image or graphic to point to other web pages/publications.

Impacting System is a data system less essential to the accomplishment of the University mission(s) and its business functions than a data system classified as Critical but without which operations would be difficult yet not severely curtailed or impeded.

Information or Data Security refers to the development and implementation of a reasonable system of measures/controls/safeguards to protect data (regardless of the medium on which it resides (e.g., tape, cartridge, disk, hard drive, etc.) and computing resources from unauthorized access, theft, removal, misuse, disclosure, and/or corruption so that data and computing resource availability and integrity is preserved. These controls 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 business continuity planning); Hardware; Software (e.g., network, operating and application system software); Data; Communications/Network; Physical and Environmental; Legal (e.g., state, federal & regulatory).

In-Line Image is a graphic that appears inside a Web document.

Institutional Data is common summary and detail data that is essential to all campuses and the President's Office and is used to reflect a single organizational picture. Much of this type of data must be combined for organizational reporting to the Commonwealth or other agency.

Institutional Records are records that contain Institutional Data.

Inter-system Communications Security refers to the controls put in place to insure that communications between computer systems at different sites is private, complete and accurate, and that unauthorized access is denied.

Interference is the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless transmission or completely eliminate it depending on the strength and location of the signal. Elevators, microwave
ovens, cordless telephones and radioactive agents can emit interference.

**Internal Records** are records created by a department for use by that department's staff only, or records created by staff to carry out their University job function(s).

**Internet** is a network of computers that allows its users to send mail or access data worldwide.

**Interoperability** refers to the condition achieved among communications systems items when information or services can be exchanged directly and satisfactorily between them and/or their users.

**Journaling** is the process of recording access (read, changes, deletions, etc.) against data so that a previous version of the data can be reconstructed. This is also referred to as logging.

**Laptop Computer** is a portable personal computer of a size suitable to rest comfortably on one's legs. A laptop is smaller than a "luggable" (portable, but not comfortably) but bigger than a "palmtop" (easily carried in one hand or a shirt pocket).

**Legal Records** are records that provide legal proof of agency authority and business transactions and the information that forms the basis for legal actions.

**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.

**Link** refers to a one-way connection from one web page/publication to another web page/publication. A link may be a "link to" or "link from" one web page/publication to another.

**Local Area Network (LAN)** refers to a several computers within in the immediate area, usually the same building or floor of a building, linked together on one network. These computers are linked together on one centrally administered network and file directory.

**Login Banner** is a screen displayed that requests an individuals logon Id/operator id and password, and which may also display other information such as date, time, site name, phone numbers, instructions, etc.

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 (e.g., Internet) to the computer system.

**Low Level Formatting** refers to the process whereby hardware file allocation tables are rewritten.
This process completely erases a drive, one sector at a time.

**Mail Bombing** refers to flooding an individual's electronic mailbox with numerous or large messages with an intent to disrupt the recipient's normal work. Not only does this negatively affect the person who is being mail bombed, but everyone on the network.

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

**Mainframe** is a large computer, usually one to which other computers and/or terminals are connected to share its resources and computing power.

**Mainframe Computer Environment** is an environment in which data processing is performed centrally on a large computer system.

**Medical Records** are records related to the physical or mental health of an individual, regardless of category (i.e., staff, student, etc.).

**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.

**Microcomputer/PC** refers to a computer in which the processing unit is a microprocessor and that usually consists of a microprocessor, a storage unit, an input channel, and an output channel, all of which may be on one chip.

**Multipurpose Internet Mail Extensions (MIME)** is a standard for multi-part, multimedia electronic mail messages and WorldWide Web hypertext documents on the Internet. MIME provides the ability to transfer non-textual data, such as graphics, audio and fax.

**Navigation Aides** are tools to help you move easily through the WWW.

**Network-based intrusion-detection systems** monitor traffic on networks and logs suspicious behavior.

**Notebook** is a portable personal computer the size of a notebook.

**Official Record** is the primary or original version of a record maintained by the University. For example, the official record of a purchase is the purchase order filed in the campus Procurement Department. Other copies of the same purchase order are considered Convenience Records.

**Official Record Custodian (ORC)** is the department responsible for maintaining the Official Record of a specific document. For example, the Human Resources area is the official record custodian for staff contracts.
Official University Web Pages/Publications or Official Web Pages/Publications are those web pages/publications on University web servers which have been created by the University, its campuses, colleges, schools, departments or other administrative offices, for University business. Official web pages/publications DO NOT include, among others, web pages/publications created by individual faculty, staff, students or student organizations. Official web pages/publications shall contain the statement, "This is an Official Page/Publication of the University of Massachusetts ________________ (Campus, unit name - e.g., English Department) and must meet University guidelines for design and content." Additionally, the word "Official" in the statement above will link to a page containing the following disclaimer:

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

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

Open Industry Standards are standards that can be used in software that allow the software to communicate with other products regardless of their architecture.

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.

Palmtop is a portable personal computer of a size easily carried in one hand or a shirt pocket.

Parallel Testing describes a test in which historical (e.g., yesterday's) transactions are processed against the preceding day's backup files at the backup site to test agreement with transactions produced under normal operations.

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".
**Permanent Records** are those records that will be kept indefinitely or at least 100 years. This designation is given to all records that the Central Administrative Services or Campus records administrator and archivist have determined as having continued historical or administrative value. Most records with a permanent retention period are transferred to the University or Campus archives when they become inactive. In a few instances, however, records with a permanent retention period are maintained in the offices of the Official Records Custodian, not the University or Campus archives.

**Personal Computer (PC)** is a general-purpose single-user microcomputer operated by one person at a time.

**Port** refers to a point at which signals can enter or leave the network en route to or from another network.

**Privacy** is the condition that is achieved when successfully maintaining the confidentiality of personal, student and/or employee information transmitted over a network.

**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.

A **Public and Private Mailing List** is an e-mail address that is an alias for a list of several e-mail addresses. Some mailing lists are simple "reflectors," redirecting mail sent to them to the list of recipients. Others are filtered by humans or programs of varying degrees of sophistication; lists filtered by humans are said to be "moderated". Public lists are available to all users of a communication system, while private lists are available to specific e-mail users.

**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).

**Reciprocal Agreement** is an agreement between two organizations whereby each organization agrees to share the other's computing facility in the event of a business disruption.

**Records** are any type of media (e.g., paper, punch card, audio, video, electronic, tape, disk, fiche, film, CD-ROM, etc.) containing data. These include books, papers, images, maps, photographs, financial statements, statistical tabulations, etc.

**Records Administrator** is the individual(s) assigned the responsibility of implementing and
monitoring the records administration and management portion of the University/Campus Records Management & Retention Program. The records administrator(s) is a job function which may be part or all of an individual's area of responsibility. Additionally, the record administrator may be the same individual(s) or a different individual(s) than the records archivist.

**Records Archivist** is the individual(s) assigned the responsibility of implementing and monitoring the records archiving and storage portion of the University/Campus Records Management & Retention Program. The records archivist(s) is a job function which may be part or all of an individual's area of responsibility. Additionally, the record archivist may be the same individual(s) or a different individual(s) than the records administrator.

**Records Conservation Board** is the agency of the Commonwealth responsible for approving actions relating to the retention and disposition of state records.

**Records Management** involves the arrangement of information/records, the process that leads to filing information/records and the equipment/facilities in which the records are stored.

**Remote Access** (dial-in, network, etc.) refers to communication with a data processing facility or its systems from a remote location or facility.

**Research Computers** are any University computers which contain 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 Designation** is the retention classification assigned to a record or group of records. Designations available are: Permanent, Until Superseded, Until Obsolete, and Specific.

**Retention Period** is the length of time a record must be maintained. Retention Period is based on the purposes for which the record was created, legal or contractual requirements/agreements, fiscal or administrative requirements of the University and/or interested external agencies, and the criticality of the data on the record.

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

**Risk Analysis** is the comprehensive study of potential disruptions to business continuity, assignment of an occurrence probability, determination of probable effects, and definition of controls that could minimize or eliminate the disruption. There are two components to risk identification: knowing your assets and identifying possible risks to them.

**Risk Management** is the balancing potential loss against the cost of reducing or eliminating
vulnerability to threats/probable disruptions.

**Risk Manager** is the senior level individual at each Campus and Common Administrative Services responsible for ensuring that risk analysis, control implementation, and BRP testing and updating are performed for all critical and impacting data systems at their campus/site.

**Rogue access points** are those installed in University facilities without coordinating with campus information security officer and network management.

**Router** is device that may be used to connect parts of a data network or two or more local area networks (LANs) to the network.

**SATAN** is a testing and reporting tool that collects a variety of information about specified hosts and networks by examining network services.

**Saturation**, in a communications system, refers to the condition in which a component of the system has reached its maximum message/data traffic handling capacity.

**Secure Sockets Layer (SSL)** is a protocol designed by Netscape Communications Corporation to provide encrypted communications on the Internet.

**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.

**Security** includes measures and controls implemented to protect data and computing resources from unauthorized access, misuse, disclosure, or corruption so that data and computing resource availability and integrity is preserved.

**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.

**Service Bureau** is a company which provides a service related to a University function (e.g., data processing, data entry, report printing, etc.)

**Service Set Identifiers (i.e., SSID)** is a unique identifier attached to the header of packets sent over an 802.11 Wireless Local Area Network (i.e., WLAN). It is primarily intended to differentiate WLANs from one another.

**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 Block** is a few lines of information about the sender of an electronic mail message or news posting.
**Signature Images** refer to the entry of a signature on a computerized document by electronic means.

**Simple Network Management Protocol (SNMP)** is an application-layer protocol designed to facilitate the exchange of management information between network devices.

**Simulation Testing** describes a method of testing the BRP in which a business disruption is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. Extensive travel, moving equipment, and eliminating voice or data communications may not be practical or economically feasible during a simulated test.

**Single Sign-on (SSO)** is mechanism whereby a single action of user authentication and authorization can permit an authorized user to access all computers and systems where they have access permission, without the need to enter multiple logon ids/operator ids and/or passwords.

**Smart Card** is any plastic card (like a credit card) with an embedded integrated circuit for storing information or verifying access identity.

**Spamming** refers to the sending of unwanted e-mail messages to a large quantity of recipients. Spamming unduly slows down a network.

**Specific** is a retention designation assigned to records that will be kept for a specified number of years.

**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.

**Structured Walkthrough Testing** describes a method of testing the BRP in which the Resumption Team members verbally "walk through" the specific steps as documented in the plan to confirm effectiveness of the plan and identify gaps, bottlenecks or other weaknesses in the plan.

**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.

**Student Records** are records related to courses, grades, housing, admissions, student disciplinary actions, non-disbursement financial aid or other academic records.

**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.

**Systems Development Life Cycle** refers to the standard steps/tasks (e.g., problem definition, business plan, conceptual design, detailed design, program coding & testing, systems testing, documentation, implementation and post-implementation review) that should be followed when developing a new or modifying an existing application system.

**Temporary Records** are records that do not fall into the other retention designations (i.e., Permanent, Until Superseded or Specific). These records should be disposed of after 6 months from the last date of entry on the record.

**Terminal** refers to a device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.

A **Third Party** in an email system refers to any individual, group of individuals, bulletin board, conference or newsgroup either within the University or at any other location worldwide 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 (e.g., 15 minutes).

**Token Security** refers to a network access procedure in which a token (i.e., a group of bits that serves as a symbol of authority) passes from one computer to another computer and the only computer allowed to transmit information is the one with the token.

**Trace Facilities** refers to methods that provide a historical record of specified events occurring in a computer system(s).

**Transmission Control Protocol/Internet Protocol (i.e., TCP/IP)** refers to the suite of communications protocols used to connect computer systems on the Internet.

**Transportable Computers** refers to computer equipment that is "light weight" and easily moved. Transportable computers include laptop, notebook, and palmtop computers.

**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.

**Tunnel** refers to a protected channel that allows individuals in one organization to go through the Internet or other public network, and reach a computer in another organization in a relatively
unfettered way.

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 may be made generally available without specific Data Custodian approval.

Uninterruptible Power Supply (UPS) is a device that protects computing equipment from the effects of transient power spikes/drops or temporary electrical outages.

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 Data System refers to any computerized or manual system which stores or processes University data.

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 of Massachusetts World-Wide Web Site or University Web Site consists of all informational pages and web based applications/databases or communications which reside on computers either purchased, leased or administered from University resources or resources managed by the University.

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.

University Records are any records 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 Records are Financial, General, Medical, Personnel, and Student, etc.

Unofficial web pages/publications - All web pages/publications that are not official web
pages/publications are unofficial web pages/publications.

**Until Superseded** is a retention designation assigned to records that are routinely updated or revised and where the previous version has no continuing value.

**User Authentication Or Authentication** is the process by which the identity of an individual and their right to access specific categories of data are verified.

**User Customizability** refers to the computer user's ability to tailor different software options to their specific preferences (e.g., web home page, language of choice, reply messages sent, message sorting, etc.)

**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.

**Vital Records** are University records which are essential to the protection of the rights of individuals or the University's rights and assets, and/or the execution of the University's public or contractual obligations.

**Web Application/Database** is any computer application or database that is accessible through the Internet.

**Web Application/Database Developer** is any individual who is creating/developing an application and/or database on the Internet.

**Web Based Communication** is communication or conversation through the Internet such as "chat groups", on-line conferencing, or class discussions.

**Web Browsers or Browsers** are software programs that are used to look at various kinds of Web resources.

**Web Consortium (W3C)** is an international industry consortium whose purpose is to lead the WWW to its full potential by developing common protocols that promote its evolution and ensure its interoperability.

**Web Page** refers to a page of information available on the Worldwide web network.

**Web Page/Publications Administrator** is any individual who is responsible for the day to day monitoring and maintenance of web pages or publications. This may be the same person as the Web Page/Publications Developer.

**Web Page/Publications Developer** is any individual who is creating/developing a page/publication for the WWW. This may be the same person as the Web Page/Publications Administrator.

**Web Page Sponsor** is the head of the entity for which the web page/publication is being developed.
Web Site/Server Administrator is any individual responsible for the support of a server attached to the Internet.

Web Server refers to a computer(s) that provides WorldWide Web (WWW) access to other computers.

Wide Area Network (WAN) refers to a geographically dispersed computer network that links multiple Local Area Networks (LANs). WANS usually cover an area larger than a single building or campus.

Wi-Fi is an industry trade name for 11 Meg 802.11b standards.

Windows registry file is a database used by the Windows operating system (e.g., Windows 2000, NT) to store configuration information.

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks defined in the standard 802.11b. WEP is designed to provide the same level of security as that of a wired network and protect wireless communication from eavesdropping.

Wireless refers to technology that permits the transfer of information between separate points using electromagnetic waves rather than a physical connection.

Wireless Access Point (i.e., WAP) - is a piece of network hardware that serves as a communications “hub” for wireless connectivity typically providing connection to the wired local area network (i.e., LAN) and therefore transmitting data between the wireless and wired networks. Access points can be connected to the wired network allowing wireless access to the campus network and connecting via radio frequency to networked devices such as laptop computers and PDAs.

Wireless Area Network (i.e., WLAN) in essence, provides the functionality of a wired local area network without the physical constraints of the wire.

Wireless Client refers to electronic equipment such as a notebook computer or handheld PDA that use wireless radio signaling to reach a network. Wireless clients work in association with wireless access points.

Wireless Infrastructure refers to wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

Wireless Networking Infrastructure refers to wireless access points (i.e., WAPs), antennas, cabling, power and network hardware associated with the deployment of a wireless communications network.

Workstation is a general-purpose computer designed to be used by one person at a time and which
offers higher performance than normally found in a personal computer (PC), especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.

**Worldwide Web (i.e., the Web or WWW)** 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.

**802.11x** refers to wireless networking standards developed by the Institute of Electrical and Electronics Engineers (i.e., IEEE).
Data Security and Classification 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.

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.

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.

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.

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.

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 Policies/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.

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.

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.

**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.
Email Communications Policy

Purpose

This policy is designed to formalize the use of electronic email for official University of Massachusetts Dartmouth communications.

Policy Statement

The University of Massachusetts Dartmouth has established email as a means of sending official information to enrolled students. To support this objective, the university provides an email account to all active University of Massachusetts Dartmouth students. The university has the right to expect that email communications will be received and read in a timely fashion.

Students may have email forwarded from their official university address to another email address at his or her risk. The university will not be responsible for the handling of email by outside vendors. Subscriptions to email lists may require that you use your university address to send messages to the list.

Students are expected to check their university email on a frequent and consistent basis to ensure they are staying current with all official communications.

Responsibilities

Computing & Information Technology Services (CITS) has overall responsibility for implementation of this policy.
The CITS Access Management team is responsible for distributing and maintaining official University of Massachusetts Dartmouth email addresses.
The content of official communications is the responsibility of the originating department.
Individuals using email are expected to adhere to the policies summarized in the "University of Massachusetts Responsible/Acceptable Use of Computing Services Summary of the University Data and Computing Use Requirements" available at http://www.umassp.edu/policy/data/acceptableuse_v3.pdf
University of Massachusetts
Responsible/Acceptable Use of Computing Services

Summary of University Data and Computing Use Requirements

Since many users share information data and technology, and because of legal and ethical requirements, all users need to be aware of their responsibilities related to data and computing at the University of Massachusetts. Please familiarize yourself with summary information below as well as the University of Massachusetts Data and Computing Policies and Guidelines for use of information technology by going to http://www.umassp.edu/policy/data/data.html. Remember that observing these guidelines will help to make computing and use of the network services more pleasant for all users. Please use the University data and computing FAQ to clarify policy, guideline, and use questions.

General
The computing resources of the University are provided to support academic and administrative users. Users should use their access to University data for approved purposes only.

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.

University data and computing users should properly create, access, use and dispose of University data based on the data's classification (e.g., Confidential, Restricted, UnClassified, etc.). See http://www.umassp.edu/policy/data/itcdatasec.html for classification information.

All computer systems accessing University data and networks must have antiviral software installed and continuously enabled so the spread of viruses within the University computer systems is prevented. Authorized users downloading software from a network or installing software from a disk/CD-ROM, must check the software for possible virus infection before they use it.

Email Accounts
All students and employees may obtain an email account. Students are free to use email for personal use. Email 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 employees' job duties or University business or operations.

The University considers a personal email message to be private however, the University has the right to look at any documents/files including emails stored, sent or received on/across University computer systems and networks if necessary for University business. Please note that due to information technology, the privacy, security, and authorship of documents and messages stored in and transmitted via electronic media cannot be guaranteed. Additionally, emails can be stored, copied, printed or forwarded by recipients. As such, you should not write anything in an email that you would not feel just as comfortable putting in a memo.

The University does not routinely monitor the content of electronic communications. The University has the responsibility and authority to access, review and release electronic information that is transmitted over or stored in University systems. The University also has the responsibility and authority to monitor individual accounts if the University determines this monitoring is necessary for legitimate administrative purposes.

Email users must use email and any other electronic communications tool in a responsible manner consistent with other business communications (e.g., phone, correspondence, etc.). Responsible email use includes: not "rebroadcasting"/sending an email to a third party obtained from another individual that the individual reasonably expects to be confidential; not posting materials that are
of a fraudulent, defamatory, harassing, or threatening nature; not sending chain emails or spamming; and not unlawfully soliciting or exchanging copies of copyrighted software via email.

**Security**
Be particularly careful of your password. Do not give your password to anyone or type your password when someone is watching. Do not write down your password or store it in batch files, automatic login scripts, terminal function keys, or in other locations where another person might discover them. Once someone has your password it is possible both to look in your directory and to use your username for malicious purposes.

Do not log on to a computer/network with your id/password and let another person use your access. Make sure you log off the computer while you step away from your desk for an extended period of time. Staying logged on leaves your id and the system vulnerable for misuse. You are responsible for all activities that take place from your account.

Although the University makes a reasonable effort to protect files stored on the university systems from being accessed by anyone other than authorized individuals, the University cannot guarantee the confidentiality of any of these files.

The University recommends the installation of personal firewalls on all University owned systems and any computer accessing University computer and network systems.

**Privacy**
The University systems may record information about each user session. Information recorded includes the username/operator id associated with the session, the login and logout dates and times, and the amount and kind of computer resources used during the session. This information is used for legitimate University purposes including issues of law, abuse, security or system managements.

When the University has reasonable belief that system security or system operation has been compromised or it has been used for unauthorized activities, the University has the responsibility and authority to review the contents of all computers including files, programs and emails.

Remember that any printouts in public places are likely to be seen by others.

**Computer Abuses**
You can expect to lose your computer account, be disconnected from the network, face disciplinary action up to and including termination, possibly be charged with criminal offenses (either by the University or third parties such as the Record Industry) or have civil action taken for computer abuses such as:

- Unauthorized access of another person's computer or email account
- Unauthorized access of University data or systems
- Misrepresenting either the University or your role at the University to obtain access to data or computer systems
- Using computing resources to access any other computer system (on or off-campus) without authorization
- Disseminating any confidential information unless such dissemination is required by the individual’s job at the University
- Deleting or copying files from another person's computer account
- Taking advantage of another user's naiveté to gain access to his/her files
- Preventing someone from using his/her account by changing the password or other tampering
- Sending offensive, harassing or threatening messages or repeated unsolicited mail
- Abusing the networks to which the University belongs
- Use of the computer or network for monetary gain, political purposes or illegal activities
- Illegal use of downloaded copyrighted materials including print, audio, and video.

- Intentionally writing, producing, generating, copying, propagating or attempting 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.

- Illegally distributing copyrighted software within or outside the University through any mechanism, electronic or otherwise.
- Any activity that interferes with the rights of others

Reports of abuse to your account can be made by contacting your system administrator. Please also note that your campus may have additional acceptable use requirements. Contact your system administrator for more information.
University of Massachusetts
Policy on Fraudulent Financial Activities

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)
- Improperities 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.
PRINCIPLES OF EMPLOYEE CONDUCT
UNIVERSITY OF MASSACHUSETTS

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.
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 inquiries 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.