**UNIVERSITY OF MASSACHUSETTS
INFORMATION TECHNOLOGY ACQUISITION POLICY**

Introduction

Campus information technology departments continue to encounter public safety, data security and system support issues when electronic equipment is attached to University/Campus networks by departments without IT's prior knowledge and review. Problems can arise with the purchase of new equipment (e.g., servers, etc.) that may not be compatible with the current IT infrastructure at the University. Problems can also arise when consultants are contracted to perform services on IT-related systems and processes without prior consultation and coordination with the IT department. Consultant actions may result in threats to the network security and the systems and processes they are reviewing. The University/Campus IT department needs to have advance knowledge of any such activity to assure system integrity and security throughout the engagement.

The IT department should be involved with the up-front evaluation and planning for new IT-related systems or services to ensure the systems are installed in compliance with University security standards. Involvement up-front will also provide the IT department with the opportunity to assess the resources and training requirements that will be required to provide the ongoing support for any new system. Some of these systems may have a direct impact on the life and safety of students and employees (e.g., emergency notification, elevator controls, etc.). System acquisitions of this nature must be evaluated in terms of network dependency and incorporate analysis of potential network disruptions, either through routine maintenance or an unanticipated event/disaster. Early inclusion of IT in the selection process for all departmental related hardware and software purchases will result in savings in terms of dollars, resources, implementations and assure the proper attention to the security aspects of the acquisition.

This Policy:

- Ensures that the IT environment to support the lease, purchase and implementation of IT related hardware and software exists;
- Identifies opportunities for cost savings through enterprise or other aggregated purchasing;
- Identifies areas of privacy or data security vulnerability or risk for which controls need to be implemented;
- Ensures that leases and acquisitions are compatible to University data and computing standards including the appropriate use and handling of Confidential data;
- Ensures that consulting engagements do not duplicate previous efforts or cause potential harm to the IT environment; and
- Ensures that IT contract, lease, and purchasing guidelines/standards (e.g., MS-ISAC, NIST, etc.) are considered.

Information technology departments have unique IT security expertise and will assist other departments with the development of security conscious bids and purchase orders.

IT departments will review bids/purchases for the following categories prior to any bid being released or before leases or purchases are made:

- IT infrastructure related (e.g., IP, switches, routers, servers, etc.),
- Mission critical IT applications or systems,
- Networked printers, copiers and fax machines
- Data or physical security related (e.g., application access control software, etc.)
- Life safety impacting (e.g., emergency notification, etc.)
- Devices monitoring critical device or infrastructure (e.g., fire detection monitoring, video cameras, etc.):
- Building control systems (e.g., HVAC, door access card readers, elevator controls, etc.) to be connected to a campus and/or President's Office network
- Any other hardware/equipment or software to be connected to/installed on a campus and/or President's Office wired or wireless network or computer system (e.g., cabling, access points, etc.) or
- Consulting related to the categories noted above.

Processes to Support Policy
To ensure that appropriate IT acquisition and lease reviews occur, campuses shall integrate the attached "Information Technology Acquisition Request for Review" form into their purchasing workflow processes.