University of Massachusetts Lowell

Policy Title:	Asset Management of Capital and Non-Capital IT Assets and Sensitive Data
Policy Number:	IT-5-135
Responsible Office:	Information Technology
Responsible Position:	ACIO, System Architecture

I. Policy Statement

Information Technology (IT) Equipment is property of the University Massachusetts Lowell and ismaintained for capital and non-capital IT assets and sensitive data. This policy summarizes the required recording and tracking of IT equipment.

II. Purpose

The purpose of this policy is to document procedures used to ensure accountability of capital ITassets and sensitive data housed on all IT assets: capital and non-capital. The university must classify, safeguard, depreciate and retire all IT equipment to ensure optimal data security, in addition to capital asset recording and tracking.

III. Scope

This policy applies to all University of Massachusetts Lowell IT assets for which the university isaccountable. This includes IT equipment purchased with State, Federal, Research Overhead, Trust, and Professional Development Funds.

IV. Definitions

Capital IT Asset: Assets with an acquisition value of five thousand dollars ($5,000.00) or greater and a useful life of at leastone year.

Non-Capital IT Asset: Assets with an acquisition value of less than five thousand dollars ($5,000.00).

V. Procedures

Purchasing

IT assets are purchased through BuyWays, the university's e-procurement system and may be distributed through contractual arrangements with third party vendors. IT equipment is delivered directly to UML IT department. The purchasing of IT equipment through ProCard is not allowed by the university. Any IT equipment reimbursement purchases must be approved by IT for encryption and data security purposes. The UML IT department has the authority to deny reimbursement of any IT assets purchase not in compliance with this policy or applicable standards.

Asset Tags

1. IT Department manual entry into Web Help Desk Ticket system includes:
    - Name, Location, Department (IT Asset Custodian)
    - Equipment and models
    - Computer Replenishment Program (CRP) status
    - IT Asset tag number
    - PO number
    - Serial number
    - Ticket number for the deployment

2. In-house UML IT barcoded asset tags created and printed from web help desk:

Tag Type	Tag Description	Equipment Type
PD	Primary Device	This is an employee's main computer system and may beeligible for the computer replenishment program
SDSUP	Supplemental Device	Used for all department purchased (not replenishment program issued) standard configuration computers
SDNSUP	Supplemental Not Supported	Used for devices such as iPadsor one-off purchases such as kindles. IT provides notice that IT support for these devices is not available or will be limited due to software, hardware, or contract incompatibilities
LD	Lab Device	Used for computer lab computers
RD	Research Desktop	Used for computers to be used for research purposes

3. Property & Asset Management capital asset tags:

Tag Type	Tag Description
C	Capital Equipment >$5,000.00 purchased with university funds
G	Capital equipment >$5,000.00 purchased with government funds
R	Capital equipment >$5,000.00 purchased with non-government research grant funds
CNT	Capital equipment >$5,000.00 that is unable to be tagged due to nature of physical equipment

VI. Responsibility

Tagging

1. IT department is responsible to physically tag all IT assets that may contain sensitive data (<$5,000.00)

2. Property and Asset Management is responsible to physically tag all capital IT assets (>$5,000.00)

Asset Management

1. UMass Lowell Property & Asset Management is responsible for communicating with UMassLowell IT regarding all capital IT equipment (>$5,000.00)

2. **Capital IT Assets**
    a. When a capital IT asset is located in the asset management system staging table, theuniversity IT department is contacted regarding the specific asset(s)
    b. The Property and Asset Management office assigns a tag and enters it into assetmanagement system and proceeds to track equipment accordingly

3. **Non-Capital IT Assets**
    a. All non-capital IT assets that may contain sensitive data are tagged and recordedthrough UMass Lowell IT department

Encryption & Data Security

1. All UMass Lowell computers are encrypted by Information Technology prior to leaving ITstorage and being provided to the end user. Encryption is provided via native OS tools, preventing anyone other than an authorized user to access data on the device.

2. UMass Lowell IT is able report on each machine's encryption status, ensuring that allcomputers are encrypted and sensitive data is secure.

3. Unique encryption keys are stored by IT for support and recovery reasons. End users cannotaccess their own encryption keys without IT support.

Employee Responsibility

1. No employee shall relinquish control of, or share their device with anyone else, including other UMass Lowell employees without written notification and approval from Information Technology. This includes but is not limited to: providing a used or second device to a new employee, relocating a desktop (tower) computer to another office, trading computers withanother employee.

2. All assets that are no longer required for essential university business shall be returned to Information Technology without exception. Assets returned to IT are redeployed or recycledat IT's discretion. IT assets shall never be recycled or removed from campus without writtenauthorization from IT.

3. No employee shall remove encryption, remove IT provided security software, remove the provided operating system, or install a different operating system without written approval from IT to do so, and in all cases encryption must be preserved.

Distribution

1. IT equipment and computers can be distributed from existing inventory, then inventory is filled with the computer originally ordered. UMass Lowell IT operates a rotating stock inventory.

Tracking

1. UMass Lowell Information Technology will record a custodian for each computer asset atthe time of deployment to the user. Any time after that, IT can identify the custodian for computer assets based on that record.

2. UMass Lowell IT through Device Management software is able to identify the most recentlogin on a particular device based on serial number of the device.

3. It is not the responsibility of UMass Lowell IT department to physically locate any givenmachine at any given time, as the university acknowledges that these are mobile assets being used by an increasingly mobile workforce. Department custodians are however, expected to monitor assets assigned to their organization and advise IT of any changes.

4. Annually, Information Technology will report on assets that have not checked in with themanagement console within the previous year and turn such list over to the asset management office for investigation.

Lost or Stolen IT Assets

1. It is the responsibility of the custodian of each device to report its loss or theft toInformation Technology immediately.

2. In the event of a lost or stolen computer, the Information Technology Security will review any specific data security concerns in regard to the lost asset in question. Identifying detailsof the computer can be provided to Campus Police if applicable.

3. Updates to the asset details are made to the record in IT's ITSM software noting that themachine has been lost or stolen.

Recycling

1. Asset is returned to UMass Lowell IT department. It is the responsibility of the asset custodian to return the IT asset to the UMass Lowell IT department after use. The IT assetrecord is updated in the Web System kept by IT department.

2. The physical machine is stored in a secure location until collected by a certified recycling vendor, approved by UMass Lowell Sustainability and IT. The vendor is required to provide acertificate of destruction to ensure proper destruction of sensitive data-storing materials.

VII. Attachments

None provided

VIII. Related Policies

None provided