FITCHBURG STATE UNIVERSITY

89 - Asset Management Policy

Issued 10/18/2022

Version 1.0

Purpose

The purpose of this policy is to ensure that an asset management program is maintained to ensure proper control, management, assessment and planning regarding information technology assets at Fitchburg State University.

Scope

The scope of this policy includes all information technology assets owned or leased by Fitchburg State University. Assets with a value in excess of $1000 must be properly tracked and tagged from acquisition through useful service lifetime to the point at which each asset is disposed of or destroyed. Additionally, there are reasons why Fitchburg State may want to keep track of equipment that costs less. In those cases, the process for tracking and tagging will be consistent with this policy.

This policy applies to all computers, laptops, servers, firewalls, routers, printers, faxes, scanners, credit card readers, swipe devices, other hardware devices and any other information technology asset that is either directly or indirectly connected to the company network (e.g., a dedicated printer connected to a computer).

Additionally, information technology assets temporarily or permanently removed from service are included in the inventory. A log of information technology assets disposed of will be kept for a minimum of 1 year from the disposal date.

Policy

•An Approved Product List must be maintained containing information technology assets that can be purchased or leased for use on the network and by staff.

•Newly acquired assets must be inventoried before they are placed into service on the company network/infrastructure.

•Only IT staff (or approved Facilities Staff) may move, connect or disconnect information technology assets, with the exception of explicit authorizations, such as mobile devices.

•Periodic inventories at a minimum on an annual basis of assets are conducted to ensure that all assets are accounted for, installed in their designated location and that no unknown assets are detected.

•As required by PCI, assets supporting credit card transaction processing are labeled to indicate: owner, contact information and purpose unless deemed out-of-scope either due to meeting PCI point-to-point encryption requirements or a component of an off-network processing solution (i.e., completely independent from the company network).

•As required by HIPAA, assets that handle Electronic Protected Health Information (ePHI) must be identified as such along with physical location in the asset inventory.

•Any “rogue” or unanticipated assets found during inventory will immediately be taken out of service and result in a security incident report.

•Any missing or unaccounted for assets will result in a security incident report and may involve the university, police and legal if a suspected/actual theft has occurred.

•Results of the periodic asset inventories are documented and made available as input to depreciation schedules, obsolescence planning and IT/general budgeting initiatives.

•All information technology asset acquisitions must follow a formal process that involves appropriate IT staff in the decision-making process.

IT Equipment Tagging Guidelines

Land-line and Cellular Phone Systems
No equipment shall be tagged except for those that meet the requirements listed above.

Servers
All servers located in the Conlon or Edgerly data centers or the main switch room in Condike Science shall be tagged regardless of price.

End-user computers
Computer systems are replaced through the University refresh program and should be tagged regardless of initial purchase price. Thin-clients and kiosk systems are not routinely refreshed and should not be tagged unless they meet the requirements listed above.

Tablets
Tablet computers are not routinely refreshed and are purchased with departmental funding and, unless they meet the requirements listed above, should not be tagged.

Printers
Shall not be tagged unless they meet the requirements listed above.

Projectors
No equipment shall be tagged except for devices that meet the requirements listed above.

Where to Attach Asset Tags
The tag should be placed in a location that does not interfere with cooling or operations, but can be easily seen and scanned, normally along the bottom or back of the device.

Inventory Reconciliation
Annually, a physical reconciliation shall be made of these assets.
* This inventory shall be done at the direction of the Chief Financial Officer.
* This work shall be performed by persons without normal access to the WiseTrack system. This requirement provides the appropriate segregation of duties between the asset software managers and reconcilers.
* If assets cannot be located, electronic means shall be used to determine where they are located.
* If assets cannot be located manually or electronically, appropriate action shall be taken as defined by state and University guidelines.

Role

Staff: Follow the formal request process for information technology asset requests. Do not move or connect/disconnect information technology assets unless explicitly authorized to do so by IT staff for troubleshooting purposes.

IT Staff: Ensure that the results of IT asset inventories are accounted for in: depreciation schedules, obsolesce planning and IT/general budgeting initiatives.

Information Security Officer: Ensure that up-to-date asset inventories are maintained; periodic asset inventories are conducted, and manage security incident activities related to information technology assets as appropriate.

References CIS

1.1 Establish and Maintain a Detailed Enterprise Asset Inventory
1.2 Address Unauthorized Assets

References PCI

PCI
Requirement 6
Requirement 12

MA 201 CMR 17:00
Section 17.04

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.