Boston University Technology Asset Management Guide

The purpose of this guide is to create an efficiently managed process for maintaining University-owned Technology Assets.

Objectives

Boston University is designing this Asset Management Guide to maintain and protect University-owned Technology Assets ("Assets"), as defined in the appendix at the end of this document. More specifically, this guide is designed to:

- Enable Asset lifecycle management, including:
    a) Inventory
    b) Device configuration
    c) Software updates
    d) Replacement planning
    e) Disposal and recycling
    f) Transfer of ownership (if necessary)
- Provide complete and accurate audit capabilities for Assets.
- Inform hardware and software purchases.
- Provide the University with information to track Assets that have been reported stolen, lost, or missing.
- Provide IS&T and other IT Support Organizations with information to aid in troubleshooting and support.
- Support compliance with applicable laws, such as, but not limited to, FERPA (Family Educational Rights and Privacy Act) and HIPAA (Health Insurance Portability and Accountability Act) that require the University to safeguard privileged or sensitive information, which may be stored on Assets.
- Ensure Assets meet Minimum Security Standards, as defined by: https://www.bu.edu/policies/minimum-security-standards/
- Support the University's Information Security Policy and Data Protection Standards: https://www.bu.edu/policies/information-security-policy/ https://www.bu.edu/policies/data-protection-standards/

Lifecycle Management

Inventory

- Assets should have an Asset Tag. Asset Tags should be attached, recorded, and tracked by the appropriate IT Support Organization.
- Assets must be assigned to an individual with full-time, permanent employment status with the University. This person is referred to as the "Asset Responsibility Owner."
    - The Asset should be assigned to this individual in a technology asset management tool.
    - Assets used by individuals in a transient role (e.g., temporary staff, part-time staff, student employees, or other, non-permanent employees) must be assigned to an appropriate Asset Responsibility Owner. The Responsibility Owner should indicate that the Asset will be used by an individual in a transient role. This individual will be identified as the "Primary Client."
    - Asset Responsibility Owner and Primary Client information should be recorded and tracked by the appropriate IT Support Organization.
- All Assets should be assigned to a campus location. The location must have a Campus and Building name or street address, along with a Floor, Office Number, and/or Cubicle Number as applicable.
    - Assets that are intended for University-related travel or a "virtual" office should still have a campus location of record. The location should indicate where the Asset will be located most often and would be located if on-site support were required.
    - Assets that are assigned to employees that work fully remotely should be assigned to the main location of their department or group.
    - Location information should be recorded and tracked by the appropriate IT Support Organization.
- Asset Responsibility Owners cannot exchange, trade, or repurpose Assets without notifying their IT Support Organization and receiving approval from their Unit Manager or Department Head.
- Assets assigned to an employee who moves to a position in another department or unit must stay with the original unit, unless approved by the original Unit Manager or Department Head.
    - Devices approved to be taken with an employee moving to another unit must be reviewed by both the originating and destination IT support groups to maintain management and supportability.

Device Configuration

- All Assets should have an asset management agent installed and/or be enrolled in a Mobile Device Management (MDM) system.
    - Asset management tools, MDM systems, or other tools, as appropriate, should be used to ensure compliance with the University's Minimum Security Standards Policy.
    - The agent and/or MDM should prevent critical or required applications, such as asset management or endpoint security solutions, from being disabled.
- Asset security controls and centrally managed policies may not be subverted, such as by, but not limited to:
    - "Jailbreaking" or "rooting" smartphones or tablets
    - Disabling macOS System Integrity Protection
    - Disabling Windows User Account Control
- Computer Names, also known as "Hostnames," must be unique for each Asset. Hostnames should start with the generally accepted abbreviation of the department to which the Asset is assigned

(e.g., IST, BUMC, CAS, etc.) with the remaining characters left up to the discretion of the individual department or unit based upon their needs.
    - Hostnames can contain up to 15 alphanumeric characters and hyphens.
    - Because hostnames are discoverable, and therefore not private, personally identifiable or potentially sensitive information should not be stored in the hostname.
- All University-owned computers should utilize University Authentication Services to provide access to the device using a BU Login Name and password.
    - Any account with privileged access to an Asset should follow the requirements stated in the Authentication Policy of the Identity and Access Management Policy.

Software Updates

- In accordance with the Minimum Security Standards, Assets should be configured to receive and install updates automatically.
- When an Asset cannot be updated automatically, an asset management system should be used to deploy updates.
- Any software, including operating systems, in use on an Asset must be appropriately licensed and supported by an organization that provides updates to remediate security vulnerabilities.
    - Where requirements prevent running fully updated operating systems and/or other software, it may be necessary to deploy compensating controls. Consult with Information Security on these cases.

Replacement Planning

- Asset inventory should be used to inform buying decisions at the time that an aging or malfunctioning Asset needs to be replaced. Departments and/or IT support groups should utilize this inventory to budget for future replacement of Assets.
- When possible, requisitioners should utilize pre-defined standards for Assets to
    - reduce the Total Cost of Ownership (TCO) of Assets,
    - help aggregate technology sped for better pricing,
    - standardize Assets for more streamlined support,
    - ensure that staff in equivalent roles have equivalent Assets, and
    - ensure that staff have the technology necessary to perform their roles.

Disposal and Recycling

- Unit Managers and Department Heads are responsible for returning any unwanted or unneeded Assets to their IT support group. These Assets may be erased and repurposed to other areas of the University.
- Prior to returning these Assets to their IT support group, managers must ensure any electronic University Records on the Asset are backed up and a record is kept in accordance with procedures defined by the University's Record Retention Policy and Scientific Research Data Policy.
- All Assets that will be disposed of must be decommissioned by the appropriate IT support group in accordance with the following guidelines:
    - Printers, Computers, and Mobile Devices may contain storage media which must be properly erased or destroyed prior to leaving BU control (e.g., returned to the vendor, sent to surplus, donated, disposed of, etc.). Drives may be disposed with IS&T's Media Destruction Service.

        - Review the University's Record Retention Policy and Scientific Research Data Policy before disposing of records.
        - Do not destroy records that are the subject of a litigation hold.
    - Assets must be disposed of in accordance with EPA guidelines using a certified service provider. Contact Facilities Management for additional assistance. https://www.bu.edu/sustainability/how-to/recycle/

Transfer of Ownership

- Prior to transferring ownership of an Asset, managers must ensure any electronic University Records on the Asset are backed up and a record is kept in accordance with procedures defined by the University's Record Retention Policy and Scientific Research Data Policy.
- Assets that are transferring ownership must be decommissioned by the appropriate IT support group. This is generally accomplished by resetting the device to a factory state. Decommissioning includes, but is not limited to:
    - Removal of BU licensed software, including the operating system
    - Removal of the Asset from any asset management and/or MDM system(s)
    - Removal of the Asset Tag

Assets Purchased with University Funds

- Approval for the transfer of ownership must be obtained from the Dean or Department Head.
- Any proceeds realized from the sale of BU-purchased equipment must return to the University.

Assets Purchased Through Grants

- For research related surplus Assets, the Dean, Chair, Director, Department Head, or Primary Investigator responsible for the grant must first gain approval for transferring or selling research property from the granting agency and the Sponsored Programs office.
- Any proceeds realized from the sale of a research-related Asset will be handled as specified by the granting agency and/or the Sponsored Programs office.

Appendix

Definitions

University-owned Technology Assets ("Assets")

Assets owned by Boston University that consist of the following equipment types:

- Desktop computers
- Laptop computers
- Smartphones
- Tablets
- Network printers
- Monitors
- Projectors
- Software installed on the above-listed devices.

For purposes of this Guide, these Assets are assumed to be valued below $5000. If you have an Asset that is valued above $5000, please contact Property Management for more specific information on how to manage and track these Assets throughout their lifecycle.

IT Support Organization

Group within a College or Department who has primary responsibility for maintenance of Assets purchased and utilized by the College or Department.

Track

Assignment of Assets to an individual and maintenance of key information about the Asset in an asset management tool, including, but not limited to:

- Unique hardware identifiers
- Asset Tag
- Purchase date
- Operating system
- Last user
- Last known IP address
- Date and time of the most recent communication with the asset management tool
- Compliance with the University's Minimum Security Standards

Tracked information is subject to the University's Access to Electronic Information Policy.

Transfer of Ownership

Can refer, but is not limited, to the following scenarios:

- When an Asset is given to a retiring or departing employee for their personal use.
- When an Asset is given to another non-profit organization (e.g., another university, a charity, etc.).
- When an Asset is sold to an entity or person.
- When the University otherwise holds no further claim on or responsibility for the Asset.