UADA Policy 915.1
Division Systems & Networking:
Access Security and Technology Asset Management Policy-Procedures

Physical Security

Purpose

The purpose of this policy is to protect information systems and the data stored and processed by them from physical hazards, including theft, vandalism, inappropriate physical access, and natural disasters.

Scope

This policy applies to all University of Arkansas System Division of Agriculture (UADA) facilities where computing devices are used in the conduct of UADA business and to all facilities in which servers and network or telecommunications equipment are installed and operated.

Policy

Data centers, server rooms, and telecommunication facilities must be appropriately designed and managed to reasonably prevent physical intrusion and unauthorized access.

- Data centers, server rooms, and telecommunication facilities must include locks and other features to reasonably prevent the bypass of physical security measures.
- Authorized persons may be granted independent access to data centers, server rooms, and telecommunication facilities. This authorization must be documented and periodically reviewed.
- Other persons may be granted temporary access to data centers, server rooms, and telecommunication facilities. They must be identified, authorized, documented, and monitored.
- Access to data centers, server rooms, and telecommunication facilities is reviewed for unauthorized access based upon an assessment of risk.
- The delivery and removal of information system components from data centers, server rooms, and telecommunication facilities must be controlled and documented.

Measures must be taken to minimize the effects on personnel and information system components in data centers, server rooms, and telecommunication facilities from reasonably anticipated hazards. Workplaces must be appropriately secured to prevent theft or damage of end-user computing devices.

- Access to workplaces should be limited to only authorized persons.
- Access to output devices (such as displays and printers) must be controlled to prevent unauthorized users from viewing or obtaining output containing restricted data.
- Computing devices must be positioned to minimize the threat of damage from physical and environmental hazards.

Procedures

The following procedures will be followed to ensure the protection of servers, networks, and telecommunications equipment:

- Data center access is limited to only authorized Office of Information Technology (OIT) and facility management personnel.
- Network and telecommunication closets will be limited to the same authorized personnel as listed above.
- Access will be controlled by secure access cards and/or limited keys.
- The data center will have dedicated air conditioning units (operating in failover status) to ensure all systems stay within environmental tolerances.
- All server, network, and telecommunication equipment will be protected from power surges and outages using adequately sized UPS units.
- The data center will be protected from extended power outages using a natural gas generator.
- The data center is protected using a clean agent (gaseous) fire suppression system.

Responsibilities

- All members of the organization are responsible for maintaining the security of their workplaces. Violations of workplace security must be promptly reported.
- All members of the organization should follow recommendations found in the Clean Desk and Clear Screen Policy.
- OIT is responsible for unit procedures for the protection of workplaces and computing devices.
- Facilities management is responsible for ensuring that appropriate facilities are available to install and operate servers, networks, and telecommunication equipment.
- Network administrators are responsible for procedures and documentation to secure data centers, server rooms, and telecommunication facilities.

Reference Documents

Clean Desk and Clear Screen Policy

Technology Asset Management

Overview

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up-to-date inventory and asset controls to ensure computer equipment locations and dispositions are well known. All lost or stolen equipment likely contains sensitive data and must be properly accounted for via property accounting. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities. This policy applies to all members of the UADA workforce:

- Employees (including faculty and staff)
- Volunteers
- Students and residents
- Extra help workers
- Contingent workers

Purpose

This policy provides procedures and protocols supporting effective organizational asset management specifically focused on electronic devices for the University of Arkansas System, Division of Agriculture (UADA).

Policy

Asset Types

The following minimal asset classes are subject to tracking and asset tagging:

- Desktop workstations
- Laptop mobile computers
- Tablet devices
- Cell phones
- Printers, copiers, and multifunction print devices
- Handheld devices
- Scanners
- Servers
- Network appliances (e.g., firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)
- Voice over Internet Protocol (VOIP) Telephony Systems and Components
- Internet Protocol (IP) Enabled Video and Security Devices
- Memory devices

Asset Value

Assets that cost less than $5,000 shall not be tracked with real property tags, including computer components such as smaller peripheral devices, video cards, keyboards, or mice. However, assets that store data regardless of cost shall be tracked through the required low-value inventory. These assets include:

- Desktop and Laptop computers
- Mobile tablets and smartphones
- Network Attached Storage (NAS), Storage Area Network (SAN) or other computer data storage devices
- Temporary storage drives
- Optical media with data stored on them including system backup data

Asset Tracking Requirements

The following procedures and protocols apply to technology asset management activities:

- All assets must have a randomly assigned Workday asset identification number with an internal asset tag number assigned and mapped to the device's serial number.
- Property accounting will ensure that the following data is tied to the asset identification in Workday for tracking purposes:
  - Date of purchase
  - Make, model, and description of asset
  - Serial Number
  - Workday asset identification number
  - Asset Identifier/internal asset tag number
  - Location
  - Type of asset
  - Owner
  - Department
  - Purchase Order number/Supplier Invoice

- Classification of asset (capital or trackable expense)
- Disposition

Prior to the deployment of computer devices, information technology staff shall assign an internal asset tag number/asset identifier to the asset and enter its information in Workday. Information Technology staff will enter in the memo of the receipt in Workday the serial number, asset tag number, and the name of the employee who will be responsible for the asset (person using the asset most of the time).

Upon termination of employment from UADA (retirement, resignation, or termination), all assets issued to departing employee must be turned in to their immediate supervisor to avoid being held responsible for the cost of the asset at the time of termination. The value of assets will be based on the remaining useful life of the asset and determined by property accounting with the formula setting the value established by State Marketing and Redistribution.

Asset Disposal and Repurposing

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus. All assets regardless of being tagged and tracked must be properly disposed of through the processes managed by property accounting according to standards established by State Marketing and Redistribution.

When disposing of any asset, sensitive data must be removed prior to disposal. Information Technology support staff shall determine what type of data destruction protocol should be used for erasure. Minimally, data shall be removed using low-level formatting and degaussing techniques. For media storing confidential or student personally identifiable information (PII) that is not being repurposed, disks shall be physically destroyed prior to disposal.

Asset Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Satisfactory examples of evidence and compliance include:

- Annual inventory of all trackable low-value and capital assets will be completed by property accounting with the assistance of business asset trackers.
- Property accounting will spot check with an in-person audit of assets at randomly selected sites.

Evidence of internal process and procedure supporting this policy for compliance with general workstation computing policies.

Reference Documents

Property Accounting (uada.edu)

Accountability and Contacts

The Chief Information Officer for UADA is charged with the responsibility to periodically review the policy and propose changes as needed.