Alvernia University

Information Technology Policy
9.1200
IT Asset Management

Contents

Document Review Log

Date Reviewed	Description of Changes
8/17/2023	Initial Draft approved by Senior Leadership Team
2/27/2024	Added Standard Computing Device section

Purpose and Scope

This policy governs the management and oversight of Information Technology (IT) equipment and software owned, leased, or licensed by the Alvernia University ("AU").

AU's Asset Management policy for Information Technology Equipment and Software promotes the efficient and lawful use of AU's information technology resources. AU's computing systems and software are intended to support its business and academic missions and to enhance the educational environment. Any use of these resources deemed inconsistent with the mission and purpose of the University will be considered a violation of this policy.

This policy applies to all AU staff, faculty, contractors, and 3rd party service providers, including student employees. Its scope includes all IT equipment and software owned by AU.

Responsibilities

Title or Role	Definition and What They are Responsible For
Chief Information Officer	Maintains and Enforces this policy.
End User	Any employee, contractor or trustee who accesses the AU network or systems containing AU data, including student employees. End users have specific responsibilities for protecting AU systems and data. These responsibilities are outlined in 9.2000, End User Responsibilities.
3rd party service provider	Any entity that provides an information system as a service to AU that is hosted outside AU, or who hosts AU data on their systems. These systems may or may not have direct integration and connectivity to the AU network and systems. These third-party systems and organizations must minimally provide equivalent protection to that provided by the AU network and systems. The specific responsibilities of 3rd party information systems providers are described in 9.4000, IT Security for 3rd Party Partners and Providers.

Policy

Regardless of funding source, this policy shall be applicable to all AU IT equipment valued at $100 or more and software, regardless of cost, and provides detailed operating procedures for the Office of Information Technology (OIT) regarding the purchase, asset management, deployment and tracking of all technology-related items.

Purchase of IT Equipment

All technology purchases, regardless of budget/account, will be reviewed by OIT prior to purchase. OIT will be responsible for verifying compatibility of requested equipment with existing technology on campus, making suggestions for alternative equipment if required.

Standard Computing Device

Full-time employees will be issued a laptop computer to perform their work duties. Employees are expected to take their laptop home every night and bring it to work with them each day. This allows all employees to work remotely if an unscheduled remote day occurs due to inclement weather or other reasons. Any exception to device type must be approved by the employee's VP on Senior Leadership Team and communicated to OIT.

Purchase of software/licensed subscriptions

Software and licensed subscription items, regardless of budget/account or cost (including freeware), will be reviewed by the OIT department prior to purchase. OIT will be responsible for verifying compatibility of requested software with existing technology on campus, making suggestions for alternative software if required.

Asset Management

OIT will include technology items in the asset management system, regardless of budget/account. Each item (computer, tablet, accessory, software license or subscription) will be assigned to an individual or department before being deployed or tracked via individual subscription software license when applicable. Individual grants will be assigned a unique asset numbering system for devices purchased by the grant. OIT shall track IT devices and software on campus in the asset management system and may locate a specific device or software license for inventory purposes. In the event of a grant audit, OIT will identify the location of devices and software licenses.

Deployment of Technology Items

All technology purchases will be shipped to the OIT office for inclusion into the asset management system and assigned a unique number prior to deployment. The item can then be assigned to an individual and tracked in the asset management inventory. When an employee relocates to a different department or terminates their employment with the University, all devices, software licenses or subscriptions assigned to that employee will be returned to the OIT department as part of the employee off-boarding process. OIT will perform a basic functionality check and cleanup of devices prior to their reissue to the successor of the vacated position. Devices will be reassigned in the asset management system.

Lost or Stolen Equipment

Employees and departments will promptly notify OIT and Campus Safety & Security if IT equipment in their charge is lost or stolen.

Consequences of Not Complying with this Policy

The greatest consequence of end user non-compliance of this policy is that it will put AU systems and data at risk and may result in additional, unnecessary costs for the institution. In addition, end users may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action resulting from violation of this policy will be coordinated with Human Resources (HR) to ensure compliance with HR policies and relevant employment law.

Policy Review

The IT Security policies should be reviewed at least annually and updated when business objectives or the risk environment change.

References and Related Policies

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

1. **NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems,** National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
2. **FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems**, Federal Information Processing Standards Publication, Computer Security Division, National Institute of Standards and Technology, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Related Policies

1. 9.1000, IT Security and Compliance Framework and Governance

Exhibits

No exhibits.