

University of Notre Dame

Information Technology Asset Lifecycle Policy

Responsible Executive: Chief Information Officer (CIO)

Responsible Office: Office of Information Technology (OIT)

Applies To: All University units, faculty, staff, student employees, contractors, affiliates, consultants, and authorized third parties

Effective Date: 09/29/2026

1. Introduction

The University of Notre Dame acquires, deploys, and manages information technology assets to support its academic, research, administrative, and operational missions. These assets include both computing hardware and software and may store, process, transmit, or enable access to University information. As institutional resources, they must be managed in a consistent, secure, and auditable manner.

This policy establishes institutional authority and lifecycle governance requirements for University-owned or University-managed IT assets, including hardware, software, and related digital assets.

2. Policy Statement

All University-owned IT assets must be managed in accordance with approved lifecycle, security, inventory, and disposal requirements.

University IT assets may not be independently acquired, transferred, retained, disposed of, or otherwise managed outside approved University processes.

All IT assets purchased, licensed, leased, or reimbursed with University funds remain the property of the University or are governed by applicable licensing agreements until formally retired or decommissioned.

3. Scope

3.1 Hardware Assets Covered

This policy applies to all University-owned IT hardware assets regardless of funding source or geographic location.

Covered assets include laptops, desktops, tablets, mobile devices, servers, and devices embedded within research instrumentation, laboratory equipment, operational technology systems, and other specialized platforms.

Vendor-provided test or evaluation devices are covered hardware assets when received, assigned, and connect to University systems, to access University data, or otherwise used for University business.

Classification as research, laboratory, embedded, operational technology, or specialized equipment does not remove an asset from governance, inventory, security, lifecycle, or disposal requirements.

3.2 Software and Digital Assets

This policy also applies to University-owned or University-managed software and digital assets including installed software, licensed applications, enterprise platforms, cloud services, Software-as-a-Service (SaaS) applications, and locally developed software.

Software assets must comply with applicable licensing, security, lifecycle, and support requirements established by the University.

Unsupported or end-of-life software must be upgraded, removed, isolated, or formally approved through the University's exception process.

3.3 Lifecycle Coverage

This policy governs IT assets throughout their lifecycle, including planning, acquisition, inventory, deployment, operational use, maintenance, reassignment, refresh, retirement, and final disposition.

3.4 Individuals Subject to this Policy

All members of the University community who use, manage, support, administer, or are assigned University-owned IT assets are subject to this policy.

This includes faculty, staff, students, research personnel, contractors, affiliates, temporary employees, and authorized third parties when using or managing University-owned IT assets.

University-owned assets assigned for research, instructional, academic, or sponsored project purposes remain subject to institutional lifecycle, inventory, security, and disposal requirements regardless of the user's employment or academic status.

3.5 Unassigned or Unused Hardware Assets

Unassigned or inactive IT hardware assets must be maintained under the custody of the designated University IT support staff for the applicable department or unit.

Departments, units, and individuals are prohibited from independently retaining, storing, or reserving unused computing devices outside the University's approved IT asset lifecycle management process.

3.6 Asset Inventory Requirements

Hardware assets must be registered and maintained within the University's authoritative system of record.

Devices or media capable of storing University data must be securely wiped, sanitized, or destroyed in accordance with approved University standards prior to reuse, transfer, reassignment, retirement, or disposal.

4. Governance and Authority

The University establishes institutional governance over IT hardware and software assets to ensure alignment with academic, research, administrative, security, financial, and compliance obligations.

4.1 Institutional Governance

The OIT, under the authority of the CIO and in alignment with University academic and administrative leadership, is responsible for establishing and maintaining governance over hardware and software asset lifecycle.

Academic units, through their respective Deans and the Provost's Office, share responsibility for ensuring compliance with this policy within their areas of authority.

4.2 Asset Records and Audit Coordination

OIT maintains the University's official system of record for IT assets.

Requests from external auditors, regulators, sponsors, or other third parties concerning University IT hardware and software assets, inventories, lifecycle records, security controls, or compliance activities must be coordinated through designated University offices. Individuals, departments, and support groups may not independently respond to external audit requests or provide official University records unless authorized to do so.

4.3 Institutional Authority

The University reserves the right to restrict use, suspend access, reclaim assets, remove devices from service, or take other protective action necessary to safeguard University systems, information, operational continuity, compliance obligations, and legal interests.

5. Lifecycle Management Requirements

5.1 Lifecycle Framework

IT assets must be managed through all approved lifecycle stages and may not bypass institutional lifecycle, inventory, procurement, security, or disposal processes.

5.2 Pre-Acquisition Evaluation

Assets must be evaluated prior to acquisition to ensure alignment with institutional security, operational, compliance, support, and financial requirements.

Pre-acquisition review should consider supported platforms, security requirements, lifecycle supportability, inventory requirements, sponsor obligations, and operational support considerations.

5.3 Procurement Requirements

Hardware purchases must follow University Computer Purchase Policy, approved purchasing systems, and preferred supplier requirements where applicable.

Software purchases must be reviewed by Information Security and Software Licensing prior to purchase or use by faculty, staff, or students to vet security and compliance risks.

Assets acquired outside approved procurement processes may not be supported, managed, connected to University systems, or reimbursed.

University-funded devices are prohibited from personal purchase, employee buyout, gifting, or any other transfer of ownership to an individual, department, organization, or other entity. These devices must remain under University ownership until they are retired and disposed of in accordance with the University's approved hardware asset lifecycle and disposal processes.

5.4 Non-Standard and Specialized Assets

Non-standard, specialized, research, embedded, or operational technology devices that cannot comply with standard University security or management controls require a formally approved exception or security variance prior to use.

5.5 Assignment and Use

Hardware assets must have defined custodianship and be safeguarded against loss, theft, misuse, unauthorized access, or improper retention.

Departments and custodians are responsible for ensuring assets remain compliant with applicable lifecycle, inventory, security, and management requirements.

5.6 Role Changes and Separation

Hardware assets must be reviewed upon role change or separation and may not bypass any stage of the approved lifecycle process ensuring hardware is reviewed, recovered, reassigned, or processed according to University lifecycle standards.

5.7 Endpoint and Software Standards

Endpoint computing devices must comply with the Hardware Asset Lifecycle and Management Standard and associated University security and management requirements.

Software assets must be properly licensed, maintained, supported, and removed or retired when no longer approved, supported, or required.

Detailed technical and operational requirements are established in applicable University standards.

6. Security Events, Legal Preservation, and Disposal

Security events involving University-owned IT assets, including hardware, software, systems, and University-managed data, must be handled in accordance with the University's Information Technology Incident Response Policy

Devices subject to litigation hold, investigation, audit preservation, or legal review may not be altered, reassigned, wiped, destroyed, or disposed of without appropriate authorization.

All hardware capable of storing University data must undergo approved data sanitization or destruction by the Service Desk prior to reuse, reassignment, transfer, retirement, or disposal.

Disposal activities must follow authorized University processes and applicable legal, regulatory, contractual, sponsor, and institutional requirements. Departments, individuals, and Embedded IT Support Groups may not independently dispose of hardware outside of approved processes.

7. Roles and Responsibilities

OIT establishes lifecycle governance, institutional standards, security requirements, and oversight for University-owned IT assets.

University units, departments, custodians, and support personnel are responsible for safeguarding assigned assets and coordinating lifecycle activities in accordance with institutional requirements.

End users are responsible for appropriate use, protection, and timely reporting of loss, theft, misuse, security incidents, or damage involving University-owned IT assets.

8. Compliance, Monitoring, and Audit

Compliance with this policy and all incorporated standards is a condition of continued access to University information technology resources and services.

The University may conduct audits, inventory reviews, reconciliation activities, compliance assessments, and security reviews to ensure alignment with institutional requirements.

9. Exceptions

Exceptions to this policy are limited and must be formally documented, business-justified, and submitted through the University's approved exception or Security Variance process.

For staff requests, the staff member's manager must approve the request and acknowledge the associated risk. For faculty requests, the faculty member's Dean must approve the request and acknowledge the associated risk. Students are not eligible to request exceptions under this policy.

Manager or Dean approval does not constitute final approval of an exception. Depending on the nature and risk of the request, additional review and approval by the Office of Information Technology Security Office or other appropriate University authorities is required before an exception is granted.

The individual receiving the exception and the approving manager or Dean are responsible for ensuring that required security measures and conditions associated with the exception are maintained.

Approved security exceptions are reviewed annually and may require renewed approval. Appropriate University leadership will be notified of security exception requests within their areas of responsibility.

Exceptions may be denied, modified, or revoked based on level of risk or failure to maintain required security conditions.

10. Policy Enforcement

Violations may result in corrective action in accordance with applicable University policies, standards, and employment guidelines.

Enforcement actions may include restriction or suspension of access to University systems, reclamation of assets, mandatory remediation activities, lifecycle correction, financial accountability for negligence or improper disposal, audit findings, or other corrective measures deemed appropriate by the University.

The University reserves the right to take protective action necessary to safeguard institutional property, systems, information, operations, compliance obligations, and legal interests.

11. Reference Documents

• Computer Purchase Policy • Information Security Policy • Information Technology Incident Response Policy • Responsible Use of Data & Information Technology Resources Policy • AI Policies and Guidelines	• International Travel Standard • Hardware Asset Lifecycle and Management Standard • Data Destruction Standard • Data Classification Standard • Endpoint Security Standard
---	--

12. History

Date: 09/29/2026

Description: Policy Issued

Appendix A – Definitions

People and Organizational Terms

Affiliate - An individual formally associated with the University but not classified as a faculty member, staff member, or student employee, including visiting scholars, emeritus personnel, volunteers, and other approved associates.

Authorized Third Party - An external individual or organization authorized by the University to access, use, manage, support, or maintain University-owned IT assets or University information under an approved agreement.

Contractor - An individual or organization performing services for the University under a contractual agreement, including consultants, vendors, and outsourced service providers.

Custodian - The individual, department, unit, or organization responsible for the day-to-day possession, management, safeguarding, and appropriate use of a University-owned IT asset.

Embedded IT Support Group - A University department, college, school, research unit, or administrative area that provides local information technology support services outside of the Office of Information Technology (OIT).

End User - Any individual authorized to use a University-owned or University-managed IT asset.

Information Technology Asset Terms

Asset Lifecycle - The complete management process for an IT asset from planning and acquisition through deployment, support, maintenance, reassignment, retirement, and final disposal.

Cloud Service - A technology service delivered over the internet rather than hosted locally by the University. Examples include Software-as-a-Service (SaaS), cloud storage, and cloud-based collaboration platforms.

Configuration Management - The process of maintaining accurate information regarding the configuration, status, and approved settings of IT assets.

Decommission - The formal process of removing an IT asset, application, or service from operational use.

Campus Workstation Program (CWP) - The University's centrally managed computer provisioning and lifecycle program provides eligible faculty and staff with a standard workstation to support their job responsibilities. The CWP establishes approved computer standards, refresh schedules, funding models, inventory management, and lifecycle management requirements to promote security, supportability, operational efficiency, and consistency across the University. Standard devices are funded through the program for eligible users, while enhanced configurations may require additional departmental funding.

Digital Asset - A non-physical technology resource owned or managed by the University, including software licenses, cloud services, electronic records, and related technology resources.

Endpoint Device - A computing device used to access University systems or data, including laptops, desktops, tablets, and mobile devices.

Hardware Asset - A physical technology device owned, leased, or managed by the University, including laptops, desktops, servers, tablets, mobile devices, and related equipment.

Software Asset - Any software application, license, subscription, platform, cloud service, or related technology resource managed by the University.

Software-as-a-Service (SaaS) - Software hosted by a third-party provider and accessed through the internet rather than installed directly on a University-owned device.

Security and Compliance Terms

Data Sanitization - The approved process of permanently removing data from a device or storage media so that the information cannot be recovered.

Disposal - The final authorized removal of an IT asset from University ownership, inventory, or operational use through recycling, destruction, transfer, sale, or other approved methods.

End-of-Life (EOL) - The point at which a manufacturer or vendor no longer provides support, updates, security patches, or maintenance for a product.

Exception - A formally approved authorization allowing a temporary deviation from a policy, standard, or requirement.

Litigation Hold - A legal requirement that prevents the alteration, deletion, destruction, or disposal of information or assets that may be relevant to actual or anticipated legal proceedings.

Security Variance - An approved exception to a specific security requirement that includes documented risk acceptance and compensating controls.

Supported Software - Software that is actively maintained by the vendor or approved support organization and receives security updates, bug fixes, or technical support.

University Data - Information created, received, maintained, stored, processed, or transmitted in support of University business, academic, research, or operational activities.