Information Technology Asset Management Policy

Office of Administration	AVP, Information Technology
Approval Authority	Executive Team
Approval Date	May 5, 2026
Last Review	
Next Review	May, 2028

1.0 Purpose

1.1. Information Technology (IT) assets are critical resources that support the academic, research, and administrative functions of Laurentian University. Effective management of these assets is essential to ensure operational efficiency, fiscal responsibility, data security, and compliance with legal and regulatory obligations.

1.2. The purpose of this policy is to establish a university-wide framework for the consistent and effective management of all IT assets throughout their entire lifecycle, from planning and acquisition to disposal and retirement.

1.3. This policy aims to:

a. Safeguard the IT assets from loss, theft, misuse, and unauthorized access.

b. Optimize the value and utilization of IT investments.

c. Ensure compliance with software licensing agreements and privacy legislation, including Ontario's Freedom of Information and Protection of Privacy Act (FIPPA).

d. Reduce operational, financial, security, and reputational risks associated with IT assets.

e. Clearly define roles and responsibilities for the management of IT assets.

2.0 Scope and Application

2.1. This policy applies to all Laurentian University community members, including faculty, staff, researchers, students, and any other individuals or entities using University IT assets.

2.2. This policy applies to all IT assets owned, leased, or otherwise controlled by Laurentian University, regardless of the funding source (including operating, capital, or research funds). Please note that personally owned devices not purchased through University procurement are not considered University IT assets.

2.3. IT assets covered by this policy include, but are not limited to:

a. Hardware Assets:

- End-User Devices (desktops, laptops, tablets, high-performance computers and peripherals)
- Servers and Data Center Equipment (physical and virtual servers, storage systems)
- Network Infrastructure (routers, switches, firewalls, wireless access points)
- Audio-Visual (AV) Equipment (projectors, video conferencing systems)

b. Software Assets (Cloud & On-Premise):

- Operating Systems
- Productivity, Security, Business, Academic, and Research Software (IT Managed software) Contracts
- Software licenses, subscriptions, and support agreements

c. Virtual Assets:

The governance requirements for virtual and intangible assets shall take effect upon formal integration into the University's IT Asset Inventory platform including but not limited to:

- University-registered domain names and digital certificates
- Other intangible assets (Copyrights, TradeMarks, Patents, Trade Secrets)

Out-Of-Scope Assets:

- Hardware Assets
  - Non-IT purchased equipment & devices
- Data and Information Assets:
  - Institutional data including student, financial, research, and employee records
  - Databases and digital media
  - (These assets will be under the responsibility of the Records and Information Management office.)

3.0 Definitions

IT Asset: Any University-owned or leased hardware, software, data, or cloud/virtual resource as defined in Section 2.3.

IT Asset Lifecycle: The complete sequence of stages an IT asset goes through from initial planning and procurement to final disposal.

IT Asset Inventory: The centralized repository of all IT asset data, maintained within Jira Service Management.

Asset Custodian: The University unit, department, or individual assigned primary responsibility for an IT asset.

IT Service Management and IT Asset Management Platform: The officially approved system, currently implemented using Jira Service Management (JSM) and Atlassian Assets, for tracking, managing, and reporting on IT assets.

Personal information refers to recorded information about an identifiable individual, as defined under FIPPA. Information identifying an individual in a business, professional, or official capacity is generally excluded unless it reveals something of a personal nature.

4.0 Principles

4.1 Stewardship and Accountability
The University is committed to responsible stewardship of public and institutional resources. IT assets shall be managed in a manner that ensures fiscal responsibility, transparency, and demonstrable accountability throughout their lifecycle.

4.2 Lifecycle Governance
All IT assets shall be governed through a structured lifecycle approach including planning, acquisition, deployment, maintenance, and secure disposal.

4.3 Security and Privacy by Design
IT asset management shall integrate security, privacy, and compliance considerations at all stages to mitigate operational, financial, and reputational risks.

4.4 Risk-Based Decision Making
Decisions related to acquisition, renewal, and retirement of IT assets shall consider risk exposure, regulatory obligations, cybersecurity posture, and business continuity requirements.

4.5 Sustainability and Environmental Responsibility
Disposal and retirement of IT assets shall comply with environmental regulations and reflect the University's sustainability commitments.

5.0 Policy Statements

Policy statements related to Software Assets and Cloud and Virtual Assets shall take effect upon formal implementation of supporting asset management processes and tools.

5.1 Procurement and Acquisition

5.1.1 All IT assets must be procured in accordance with the University's Procurement Policy.

5.1.2 IT Services must be consulted prior to the acquisition, renewal, or material modification of hardware, enterprise software, or cloud services to ensure compatibility, security, licensing compliance, integration feasibility, and alignment with institutional architecture standards.

5.1.3 A security and Privacy Impact Assessment (PIA) is required prior to the acquisition, implementation, subscription, renewal, or significant enhancement of any IT asset, consisting of on premise software and cloud based services, that will store, process, or transmit sensitive or personal information.

5.1.4 PIAs should be initiated as early as possible in a project's lifecycle, particularly for new initiatives or changes to existing information management processes or systems that involve personal information.

5.1.5 The University remains accountable for personal information in its custody or control under FIPPA, regardless of whether that information is stored, processed, or managed by a third-party vendor or contractor. All engagements with third parties involving personal information must uphold the University's obligations under FIPPA.

5.1.6 No business unit may independently procure enterprise software or cloud services that duplicate existing centrally supported solutions without review and approval from IT Services.

5.2 Registration and Inventory

5.2.1 All IT assets falling within the scope of this policy must be registered in the University's central IT Asset Inventory within **Jira Service Management (JSM)** upon acquisition and prior to deployment.

5.2.2 The IT Asset Inventory in JSM shall, at a minimum, record the following for each asset: a unique identifier(assigned by JSM), description (make, model, serial number), asset custodian, physical location, purchase date, and warranty/service contract information.

5.2.3 Asset Custodians are responsible for notifying IT Services of any changes to the status, location, or ownership of assets under their care, which will be updated in the JSM record.

5.3 Deployment and Use

5.3.1 All IT assets must be used in a responsible manner that complies with the University's Electronic Services Acceptable Use Policy and all other applicable policies.

5.3.2 Asset Custodians are responsible for the physical security of assets assigned to them and must take reasonable precautions to prevent theft, damage, or loss.

5.3.3 Any loss or theft of an IT asset must be reported immediately to Campus Security and IT Services.

5.3.4 While personally owned devices are not considered University IT assets, accessing or handling personal information in the custody or control of the University on such devices is not permitted unless explicitly authorized by IT Services in consultation with the Privacy Office. Such authorization shall be granted only in exceptional circumstances and must be supported by appropriate safeguards to protect the information, consistent with the University's obligations under FIPPA.

5.4 Maintenance and Support

5.4.1 IT Services is responsible for the maintenance and support of all technology assets.

5.5 Asset Disposal and Retirement

5.5.1 No IT asset may be disposed of, sold, donated, or discarded without the express approval of IT Services.

5.5.2 All data storage devices (e.g., hard drives, SSDs, USB Keys, external drives) must be securely sanitized or physically destroyed by IT Services before the asset is disposed of, in accordance with University data security standards.

5.5.3 Disposal of IT assets must comply with all relevant environmental regulations and sustainability best practices.

5.5.4 Personal information must be destroyed in a manner that prevents its reconstruction or retrieval. Reasonable steps must be taken to protect the security and confidentiality of personal information during storage, transportation, handling, and destruction. Disposal records must be maintained, detailing the authority, information disposed of, approval, method, and date, without containing personal information.

6.0 Roles and Responsibilities

6.1 **AVP, Information Technology:** Is the Policy Owner, responsible for the strategic oversight, implementation, and review of this policy.

6.2 **Information Technology Department (IT):** Is responsible for the day-to-day administration of this policy, including maintaining the central IT Asset Inventory, managing the asset lifecycle processes, and providing guidance to the University community.

6.3 **Deans, Department Heads, and Managers:** Are responsible for ensuring that their units comply with this policy and for the budgetary management of IT assets within their areas.

6.4 **Asset Custodians (Faculty, Staff, etc.):** Are responsible for the proper use, handling, and physical security of the IT assets assigned to them.

6.5 **Information and Privacy Officer:** Is responsible for providing privacy oversight and guidance in the implementation of this policy, including advising on privacy impact assessments and ensuring that the University's obligations under FIPPA are met with respect to the acquisition, use, and disposal of IT assets that involve personal information.

7.0 Compliance and Enforcement

7.1 Compliance with this policy is mandatory.

7.2 Failure to comply with this policy may result in the revocation of access to Laurentian University IT resources and may be subject to disciplinary action in accordance with existing University policies and collective agreements.

8.0 Related Policies, Standards, and Legislation

- Procurement Policy
- Policy on Access to Information & Protection of Privacy
- Electronic Services Acceptable Use Policy
- Access to Electronic General and Personal Information
- Records & Information Management Policy

- Freedom of Information and Protection of Privacy Act (FIPPA), Ontario
- Accessibility for Ontarians with Disabilities Act (AODA)

9.0 Policy Review

This policy shall be reviewed every two years, or more frequently as required by changes in technology or legislation, under the direction of the AVP, Information Technology.