Responsible Unit	Technology Services
Last Reviewed/Updated	April 2024
Approving Sector Head	Vice-President, Finance and Administration and Chief Financial Officer
Policy	Acceptable Use and Security of Information and Systems

Purpose

This policy safeguards the ongoing operation of Acadia University from preventable technology failures by establishing methods to maintain the confidentiality, integrity, and availability of information and information systems (collectively “Information Assets”).

The university provides access to Information Assets to its employees, students, contractors, and partners (collectively “Users”) to enable their work and enhance their productivity, with the understanding the Information Assets must be used in a responsible, ethical, respectful way, and in compliance with applicable legislation, regulation, and policy.

This policy sets the responsibilities for the development and governance of IT policy and is the foundation for all other IT Guidelines and Standards. It requires a recognized cybersecurity management framework to be followed.

Scope

The policy applies to all Information Assets owned, leased, or provided by the university and all information used to conduct the operation of the university. It applies to all users of Information Assets, including employees, students, alumni, board and senate members, volunteers, guests, and contractors. It encompasses all activities related to the use and security of Information Assets across all departments and sectors within the University. The policies and guidelines herein are applicable in various environments, including on-campus operations and remote or online activities.

Should there be a conflict between this policy and any legally binding agreement or legislation the applicable agreement or legislation will govern.

Definitions

Information Assets is all information, data, or technology that is owned, managed, or handled in the operation of the university.

A **User** is any person or entity that accesses Information Assets.

IT Guidelines document the purpose and methods of delivery of IT services, e.g., laptop replacement or password management.

IT Standards document the technical objectives and metrics of IT services, e.g., laptop specifications or minimum password length.

IT Advisory Committee provides support to the CIO with membership from university leadership, faculty, students,

CIO refers to the senior administrator responsible for IT Strategy and Programs.

Responsibilities

The **Board of Governors** is responsible for approval of this policy and approval of the IT risk tolerances proposed by management.

The **President** is responsible for approval of the IT risk framework and residual risk levels.

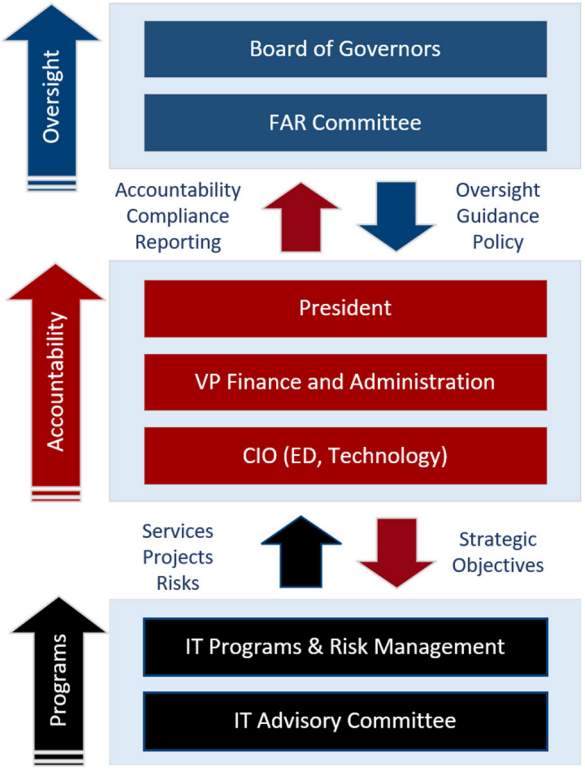
The **Vice-President, Finance and Administration and Chief Financial Officer** is the sponsoring executive responsible for approval of individual risks, risk treatment plans, and ensuring programs, including cybersecurity, meet approved risk tolerances.

The **CIO (Executive Director, Technology)** is responsible for recommending and maintaining policy and associated Guidelines and Standards; providing guidance on compliance with the policy; implementation of service programs, including information security, IT risk management; and facilitating community review of programs and risk through the IT Advisory Committee.

The **IT Advisory Committee** is responsible for reviewing guidelines, standards, risks, and proposed projects, providing guidance to the CIO on strategic value and potential issues.

Users are responsible to be aware of the policy and follow its directives.

Governance Diagram



Policy

1. Acceptable Use

    1.1 Information Assets are property of Acadia and must be used in accordance with applicable laws, collective and contractual agreements, university policies, standards, and guidelines.

1.2 Users are encouraged to use the university's Information Assets to further the mission and goals of Acadia University.

1.3 Users should use their own technology for personal work, however limited use of the network, systems, and devices, but not information or data, for personal reasons is permitted provided all Acadia policies are followed.

1.4 Acadia cannot and does not make guarantees regarding the security or privacy of personal documents and files.

1.5 Information Assets may not be used for unethical or unlawful purposes or personal gain, including copyright infringement, libel, slander, fraud, defamation, plagiarism, intimidation, forgery, impersonation, illegal gambling, soliciting, and computer tampering.

1.6 Access to Information Assets is controlled through accounts and passwords issued to Users for only their access. Users are restricted to accessing or purchasing only technology, devices, applications, or services that are formally authorized and approved by Technology Services.

1.7 Information Assets are intended to be used by only the User granted access, who is responsible for appropriate care of the Information Assets.

1.8 Users must always protect Acadia's Information Assets, keeping them physically and software secured when not in use, and under the control of the user.

2. Privacy and Personal Rights

2.1 All IT employees must be trained on the privacy requirements of their job.

2.2 IT privacy incidents must be promptly reported to the university Privacy Officer.

2.3 All users of the University's Information Assets are expected to respect the privacy and personal rights of others. Unauthorized access to the account, email, data, programs, or files of another user is prohibited.

2.4 While the University does not generally inspect User data, it reserves the right to access and review such information under certain conditions including, but not limited to:

2.4.1. Ensuring the integrity of Information Assets and protection of university property;

2.4.2. Investigating performance deviations and system problems;

2.4.3. Conducting investigations regarding security, illegal activity, or activities that may contravene this policy, any other university policy, guideline, or regulation, any contractual agreement, or any federal or provincial law;

2.4.4. Carrying out urgent operational requirements during an employee's absence where alternative arrangements have not been made;

2.4.5. Compliance with the law.

2.5 Access to user data on University Information Assets must be approved by the Approving Sector Head for This Policy, or their delegate.

3. Security

3.1 A cybersecurity program must be maintained, and reports provided regularly.

3.2 Cybersecurity Awareness Training must be provided, monitored, and reported.

3.3 A recognized Cybersecurity Framework must be followed.

3.4 To maintain the security of Information Assets, Users intending to conduct university business using systems other than those systems issued by Acadia Technology Services must do so in accordance with the information security guidelines and standards established by the university.

4. General

4.1 All purchases and projects involving IT must be approved by the CIO.

4.2 IT Risks will be monitored, reported, and addressed as soon as possible.

4.3 Users who become aware of a breach of the policy must bring the breach to the attention of the CIO or their identified delegate for appropriate action.

5. User Compliance

5.1 When you use Acadia Information Assets you agree to comply with this policy, as well as the Guidelines and Standards established under this policy.

5.2 The Policy will be available for reference along with other university policies.

5.3 All users must be aware of their responsibilities as defined by this Policy.

5.4 Exceptions to the Policy must be approved by the President of Acadia University.

5.5 Policy violation requires appropriate action by Department Heads, Deans, Vice-Presidents, and Human Resources.

6. Implementation

6.1 The policy will be reviewed annually and updated as needed to reflect changes in the environment.

6.2 Changes in the policy will be communicated to campus.