POLICY STATEMENT

Policy Name	**Information Technology Security**		
Policy #	**806**	Category	**Information Management**
Policy Sponsor	**Associate Vice-President, Information Technology Services**	Previous Revision Date	**June 4 2019**
Policy Approved by	**President & CEO**	Issue or Revision Date	**May 2024**
Procedures Approved by	**CFO & Vice-President, Administrative Services**	Review Date	**May 2029**

PURPOSE

The purpose of this policy is to:

1. Protect the confidentiality, integrity, and availability of Saskatchewan Polytechnic (Sask Polytech) information and associated Information Technology (IT).

2. Provide support for Sask Polytech IT security in accordance with business requirements and applicable laws and regulations.

3. Define the roles and responsibilities of individuals and organizational entities involved in IT security.

4. Ensure the reliable operation of Sask Polytech's IT systems.

5. Establish an organization-wide IT security framework.

SCOPE

This policy applies to all information, computing, applications, communication, and networking resources connected to or associated with Sask Polytech, and the users of said resources, including employees and students. This policy also applies to third parties and members of the public who contract or engage with Sask Polytech.

GUIDING PRINCIPLES

Sask Polytech is committed to the following guiding principles in its oversight and implementation of IT security:

1. Implementing IT security which facilitates and enables Sask Polytech's mission, vision, and strategy.

2. Maintaining individual privacy in accordance with all laws and regulations.

3. Having clearly defined IT security responsibilities and accountabilities.

4. Providing cybersecurity training to enable employees and students to protect IT and information assets.

5. Implementing security controls that are cost-effective and in proportion to the risks and value of the assets that need to be protected.

6. Integrating IT security into all necessary aspects of Sask Polytech's planning, development, and operations with a multi-disciplinary and comprehensive approach.

7. Acting in a timely, coordinated manner to prevent and respond to security incidents.

8. Periodically assessing IT security to ensure that adequate measures are in place to protect the assets of Sask Polytech.

POLICY

1. Sask Polytech must be able to share information to deliver on its mandate, which requires that security measures be implemented which enable appropriate information exchange in support of this mandate.

2. Sask Polytech shall protect its information and IT against unauthorized access, hazards, and other threats or attacks that could result in financial, legal, or reputational harm to Sask Polytech, its users and third parties.

3. Users of Sask Polytech IT are personally responsible for the protection of information assets under their control and shall respond appropriately to protect the confidentiality, integrity, and availability of the assets.

4. All Sask Polytech employees and students and others granted use of Sask Polytech IT services and resources, are expected to be aware, understand, follow, and report violations of all Sask Polytech IT policies and related frameworks, guidelines, procedures, and processes.

5. Sask Polytech IT Services shall be responsible for setting specific policies, guidelines, procedures, frameworks, and requirements using the NIST Cybersecurity Framework as guidance to lower the risk and impact of cybersecurity breaches and IT business disruptions.

6. Sask Polytech shall educate employees, students, and others granted access to IT services and resources on the need for appropriate cybersecurity, and on protecting themselves against a breach of their systems and unauthorized access to their personal information or Sask Polytech information assets.

DEFINITIONS

N/A

RELATED POLICIES/DOCUMENTS

Appropriate Use of Information Technology 801
Code of Conduct Policy 703
National Institute of Standards and Technology, Framework for Improving Critical Infrastructure (see our Collaborate site)

APPLICABLE LEGISLATION OR REGULATIONS

The Local Authority Freedom of Information and Protection of Privacy Act