POLICY STATEMENT

Policy Name	**Information Technology Security**		
Policy #	**806**	Category	**Information Management**
Policy Sponsor	**Associate Vice-President, Information Technology Services**	Previous Revision Date	**November 7, 2012**
Policy Approved by	**President & CEO**	Issue or Revision Date	**June 4, 2019**
Procedures Approved by	**CFO & Vice-President, Administrative Services**	Review Date	**June 2024**

PURPOSE

The purpose of this policy is to:

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

2. Provide management direction and support for IT security in accordance with business requirements and relevant laws and regulations;

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

4. Ensure the reliable operation of Saskatchewan Polytechnic's IT, meeting the requirements of all Saskatchewan Polytechnic stakeholders; and

5. Establish an organization-wide IT security framework.

SCOPE

This policy applies to all Saskatchewan Polytechnic information, computing, communication and networking resources connected or associated to Saskatchewan Polytechnic and the users of these resources, including faculty, staff, and students. This policy also applies to third-parties contracted with Saskatchewan Polytechnic and members of the public.

GUIDING PRINCIPLES

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

1. Developing and implementing IT security that facilitates and enables Saskatchewan Polytechnic's mission, vision, and strategy;

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

3. Clearly defining IT security responsibilities and accountabilities;

4. Providing cybersecurity training to enable employees to protect 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 every aspect of Saskatchewan Polytechnic'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; and

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

POLICY

1. Saskatchewan Polytechnic needs to share information to deliver on its mandate. Therefore, security measures shall be implemented that enable appropriate information exchange in support of this mandate.

2. Saskatchewan Polytechnic 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 Saskatchewan Polytechnic, its users and third-parties.

3. Users 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 Saskatchewan Polytechnic faculty, staff, students and units, and others granted use of Saskatchewan Polytechnic IT services and resources, are expected to be aware, understand and follow all Saskatchewan Polytechnic IT policies and related frameworks, guidelines, procedures and processes.

5. Saskatchewan Polytechnic Information Technology Services (ITS) shall be responsible for setting the specific policies, guidelines, procedures, frameworks, and requirements to lower the risk and impact of cybersecurity breaches and IT business disruptions.

6. Saskatchewan Polytechnic shall educate faculty, staff, students and units on the need for appropriate cybersecurity, and on protecting themselves against breach of their systems and unauthorized access to their personal information or Saskatchewan Polytechnic information assets.
7. The Director, Information Security, will provide oversight and be accountable for the implementation of the framework, and engage appropriate leaders and governance groups for advice.

8. If any individual reasonably suspects or believes that a security incident has occurred, they will follow the SP incident response process and log the incident with the SP Helpdesk.

9. Any individual or unit found to operate in violation of this policy may be held accountable for remediation costs associated with a resulting cybersecurity incident or other regulatory compliance penalties, including but not limited to financial costs, legal fees and other costs.

10. Faculty, staff, students or units who violate this policy and supplemental procedures may be subject to disciplinary action.

DEFINITIONS

N/A

RELATED POLICIES/DOCUMENTS

Appropriate Use of Information Technology (Policy #801)
Code of Conduct Policy (Policy #703)
Saskatchewan Polytechnic Information Cybersecurity Framework (see ourCollaborate site)
National Institute of Standards and Technology, Framework for Improving Critical Infrastructure (see ourCollaborate site)

APPLICABLE LEGISLATION OR REGULATIONS

The Local Authority Freedom of Information and Protection of Privacy Act