SAIT

AD.1.1.3 PRIVACY INCIDENT RESPONSE	
Section:	Administration (AD)
Subject:	Organization of the Institution
Legislation:	*Access to Information Act (*RSA 2024, c A-1.4); *Post-Secondary Learning Act* (SA 2003 cP-19.5); *Protection of Privacy Act* (SA 2024, c P-28.5); *Protection of Privacy (Ministerial) Regulation (143/2025).*
Effective:	May 21, 2026
Revision:	

PROCEDURE

APPROVED: _____

President and CEO

POLICY

The policy of the Board of Governors is to comply with the *Protection of Privacy Act* (POPA) and the *Access to Information Act* (ATIA).

PROCEDURE

DEFINITIONS

Personal information — Recorded information about an identifiable individual and includes, but is not limited to, name, residential address and phone number, personal email address, sex (sex assigned at birth), age, gender identity, title, pronouns, sexual orientation, marital or family status, religious affiliation, Indigeneity, ethnicity, disability status, languages spoken, immigration status, identification number, education and employment history, health information including documentation of approved accommodations for physical or mental disability, an individual's personal views or opinions and information about an individual's financial matters.

Privacy breach — Privacy incident involving a loss or unauthorized access or unauthorized disclosure of personal information.

Privacy incident	Any event that compromises the confidentiality, integrity, or availability of personal information.
Real risk of significant harm (RROSH)	Any event where personal information is lost, inappropriately accessed, or shared, and the privacy breach poses a real risk of significant harm to an affected individual.

GOVERNING PRINCIPLES

1. SAIT is committed to safeguarding personal information in its custody or control by taking all reasonable precautions and security measures to mitigate against such risks such as unauthorized access or unauthorized disclosure;

2. This procedure ensures that all privacy incidents are reported, assessed promptly and documented in SAIT's official privacy incident reporting system.

PROCEDURE

A. Reporting Requirements

1. All employees, contractors, volunteers and third-party service providers or vendors must report any suspected or confirmed privacy incidents immediately.

2. Privacy incidents must be reported through the privacy incident reporting system on SAIT's online self-service portal (mySAIT).

B. Initial Assessment

1. The Access and Privacy unit, Office of General Counsel, will assess the potential risk and severity of the privacy incident, in accordance with the *Protection of Privacy Act* (POPA). The assessment will determine if there is a real risk of significant harm (RROSH) to affected individuals.

2. The Access and Privacy unit, Office of General Counsel, will consult with the Information Technology Services (ITS) department to investigate systems or potential data exposure, as necessary.

C. Notification

1. Affected individuals will be notified as soon as reasonably practicable if there is a real risk of significant harm (RROSH), in accordance with the *POPA*.

2. Where an assessed privacy incident involves a RROSH to an affected individual(s), SAIT must notify the Office of the Information and Privacy Commissioner (OIPC) and the Minister of Technology & Innovation, as required under the *POPA*.

D. Non-compliance

1. Failure to comply may result in disciplinary hearings under procedure HR.4.4.1 Corrective and Disciplinary Action and/or legal or regulatory penalties under the POPA.

POLICY/PROCEDURE REFERENCE

AD.1.1	Privacy policy
AD.1.1.1	Personal Information procedure
AD.1.1.2	Privacy Impact Assessment procedure
AD.1.1.4	Privacy Complaints procedure

PROCEDURE