SAIT

AD.3.2.1 RECORDS MANAGEMENT	
Section:	Administration (AD)
Subject:	Records Management
Legislation:	*Alberta Evidence Act* (RSA 2000 cA-18); *Copyright Act,* R.S.C., 1985, c.C-42; *Electronic Transactions Act* (SA 2001 cE-5.5); *Financial Administration Act* (RSA 2000 cF-12); *Freedom of Information and Protection of Privacy Act* (RSA 2000 cF-25); *Government Emergency Management Regulation* (AR 248/2007); *Health Information Act* (RSA 2000 cH-5); *Historical Resources* Act (RSA 2000 cH-9); *Personal Information Protection Act* (SA 2003 cP-6.5); *Public Service Act* (RSA 2000 cP-42); *Records Management Regulation* (AR 224/2001); *Trade-marks Act,* R.S.C.1985, c.T-13.
Effective:	May 18, 2016
Revision:	September 1, 2016 (reformatted); May 23, 2018

PROCEDURE

APPROVED: _____

President and CEO

POLICY

The policy of the Board of Governors is to establish a records management practice to effectively manage the lifecycle of all SAIT's recorded information and records, from their creation or receipt, regardless of format, for the lifecycle of the record.

PROCEDURE

DEFINITIONS

Classification scheme — A system of organizing records based on function and subject. Designed to support ease of retrieval, storage, access and disposition through consistency in description and control. Classification and retention work together to provide a complete summary of the records, what they are, where they are being held and how long to be retained.

Digital records — Records created, communicated and maintained by means of computer technology. Records may be "born digital" (created using computer technology) or they may have been converted

	into digital format from their original format (for example, scans of paper documents).
Disposition	The final administrative action taken with regards to a record, including its destruction, transfer to another entity or permanent preservation.
Electronic record	Records entered, created, manipulated and/or stored on electronic media that show evidence of actions and decisions made in the normal course of business. Examples include but are not limited to electronic mail (email), electronic document exchange (fax), word processing, spreadsheets, database files, web pages, voice mail, text messages and audio and video files.
Hard copy	Any record that exists as a physical object or form.
Historical	Information that serves to record historically significant functions, activities or events.
Information	Data or knowledge that is communicated in the course of business.
Integrity	The accuracy and consistency of the record over its entire lifecycle.
Legal hold	A process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated, threatened, pending or in progress.
Lifecycle	Distinct phases of a record's existence, from creation to final disposition.
Official record	Original document from which subsequent copies might be made.
Record	Information created, received and maintained as evidence by an organization or person, in pursuance of legal obligations or in the transaction of business. A record may be in any form. This includes notes, images, audio-visual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but

PROCEDURE

	does not include software or any mechanism that produces records.
Records management	Field of management responsible for the efficient and systematic control of the record lifecycle.
Retention and Disposition Schedule	A legal instrument that describes the records under the control of a public body and that specifies how long and where the records must be kept as they progress through the phases of their life cycles, the format in which the records must be stored, and what their final disposition will be (destruction or archival preservation) at the end of their life cycles. This is also referred to as the "Retention Schedule".
Scholarly activity	Scholarly activity in the polytechnic context is any activity that involves the intentional creation, integration and/or transmission of knowledge with a view to informing professional practice, contributing to the state-of-practice within a field and/or impacting the broader external environment. Applied research is one form of scholarly activity at SAIT.
Transitory record	A record that has only immediate or short-term usefulness and will not be needed in the future. Transitory records contain information that is not required to meet legal or financial obligations or to sustain administrative or operational functions and has no historical value.
Vital record	A record that is essential for preserving, continuing or reconstructing the operations of SAIT and protecting the rights of SAIT, its employees and its stakeholders in the event of a disaster.

GOVERNING PRINCIPLES

1. Establishing recordkeeping as a systematic part of SAIT's business operations is essential to ensuring records are identified, captured, managed and retained in an accessible and usable format that preserves the integrity of the record over time.

2. The Classification Scheme and Retention and Disposition Schedule (the "Retention Schedule") is a living document and must be maintained and updated to reflect changes in SAIT's operational, fiscal, policy and regulatory requirements.

3. The following recordkeeping principles apply to SAIT's business records:

   a) Accountability

      i) SAIT is the owner of all recorded information related to the institution and to all of its organizational units.

   b) Transparency

      i) SAIT will actively document, in an understandable manner, the processes and activities of the recordkeeping practice, and will make the documentation available to all record custodians. Record definitions and terms must be defined consistently and be accessible across SAIT.

   c) Integrity

      i) Records must be maintained and managed over time in an auditable and traceable manner.

      ii) The ability to prove that records are authentic, meaning that the origin, time of creation or transmission and content are what they are supposed to be.

   d) Protection

      i) SAIT records must be protected from unauthorized access and modification. In particular:

         - Appropriate record security measures must be adhered to at all times to ensure the safety, quality and integrity of SAIT records.

         - A person who receives authorization for access to records cannot transfer the authorization to another individual.

         - Records in electronic format must be protected by appropriate electronic safeguards and/or physical controls that restrict access to only authorized users.

- Records in hard copy format must be stored in a manner that restricts access to only authorized users.

ii) Record custodians leaving SAIT or changing positions within the institution are to leave all records in their previous school/department.

iii) Records must be accessed and used only for their intended purpose. Records must not be accessed or manipulated for personal gain or out of personal interest or curiosity.

e) Compliance

i) SAIT will manage its records in accordance with applicable legislation, regulations, policies and procedures, in order to meet operational, legislated, financial and historical requirements.

ii) All record custodians must:

- Comply with the *Freedom of Information and Protection of Privacy Act* (*FOIP Act*) and SAIT's FIRST principles when accessing SAIT's records.

- Respect the privacy of individuals whose record is being accessed. No subsequent disclosure of personal information contained in recorded information may be made. Disclosure includes but is not limited to verbal references or inferences, correspondence, memoranda or sharing of hard copy or electronic records.

- Comply with the current Payment Card Industry (PCI) security standards

f) Availability

i) SAIT will ensure records are available in a timely, efficient and accurate manner when retrieval is requested.

ii) Access to records relies on having an efficient set of tools and methods to make the retrieval and organization of records successful at all levels of SAIT. This includes:

- A routine approach for capturing metadata, which must be documented and utilized in all applicable systems.

- Routinely backing up electronic information to ensure restoration in the event of a disaster, a system malfunction or data corruption.

g) Retention

i) To ensure records are retained only for as long as they are needed, retention of records will be scheduled according to operational, fiscal, legal and historical requirements.

- Records are consistently retained for the appropriate amount of time.
- Records that reflect SAIT's history should be preserved for the life of SAIT.
- The Retention Schedule addresses what business records must be retained for what length of time.
- The Retention Schedule excludes records created, received and retained by employees as part of their activities resulting from applied research agreements and proposals, or from scholarly activities.
- Transitory records will be identified and managed according to established procedures.

h) Disposition

i) Disposition of records at SAIT will be in accordance with the identified time frames found in the Retention Schedule. Secure and appropriate disposition for records will be applied.

- Disposition of records will cease in the event of a legal hold, audit process or *FOIP Act* request.
- Disposition of records will follow an auditable and documented approval process.
- Records in all media are disposed of in a manner appropriate to the information content and retention policies.

4. SAITs CFO and vice president, finance and corporate services, is responsible for the overall administration of this policy and accompanying procedures

A. Scope

1. The practice of records management falls to record owners, trustees, stewards and custodians at SAIT and applies to information created and received in the course of business, regardless of format or medium of storage.

2. It includes all records such as email, texts, websites, social media, databases and business records.

3. This applies to records created and managed in-house and off-site.

B. Records Management Roles and Responsibilities

1. Record custodians may act in one or more specific roles when creating, collecting, maintaining, transmitting, accessing or using records produced by the institution and must understand and fulfill the responsibilities of their roles.

2. SAIT will establish and manage records using the principles of stewardship and record sharing. Roles and responsibilities have been established to promote and safeguard the integrity, security and appropriate access to records**.** These roles include:

Record custodian	All SAIT employees, contractors, sub-contractors and agents are considered record custodians. Record custodians need and use SAIT records as part of their assigned duties. Record custodians may act in one or more specific roles when creating, receiving, collecting, reading, copying, querying, updating, maintaining, transmitting, accessing or using paper or electronic records and must understand and fulfill the responsibilities of their roles. All record custodians have an obligation to properly document what they do by creating accurate records of their activities and by ensuring that the appropriate records and information relating to business decisions are retained.
Record owner	SAIT is the owner of all records that SAIT creates and receives, and determines how records will be shared. Schools/departments are responsible for particular elements and/or aspects of the records**.**

PROCEDURE

Record steward	A person within the school/department responsible for all queries and/or issues related to records. A record steward is a business user with expert knowledge of business processes and how records are used within those processes. The record management activities assigned to the record steward may be assigned or delegated by a record trustee.
Record trustee	Accountable for the security, privacy, definitions, quality and compliance with record management policies and standards for a specific school/department. Each trustee is responsible for the trustee's assigned records, and for approving requests for access to those assigned records. While most records will eventually be stored electronically, this procedure covers the use of records at all stages of the lifecycle, whether electronic or in print.
Records Management Services	The Records Management Services unit, Finance department, is responsible for all aspects of records management, including managing and maintaining the Retention Schedule, and designing, implementing and providing training on records management programs and operations.

C. Security Classification of Records

1. All records must be assigned a security classification that identifies ownership and control. Records at SAIT fall into one of the four following categories:

Security Classification	Description	Examples of Records	Examples of Risk Impacts
Unrestricted	Records created in the normal course of business that are unlikely to cause harm. They are available to the public, employees and contractors, sub-contractors and agents working for SAIT.	Job postings, SAIT email addresses, course/program descriptions, etc.	Little or no impact

Protected	Records that are sensitive outside of SAIT and that could affect service levels or performance. Authorized access (to employees, contractors, sub-contractors and agents) is on a need-to-know basis for business-related purposes.	Grades, records of birth, personal contact information other than SAIT email addresses, etc.	Disruption to business if not available
Confidential	Records that are sensitive within SAIT and that could cause serious loss of privacy, competitive advantage, loss of confidence in SAIT programs or damage to partnerships, relationships and reputation. They are available only to a specific function, group or role.	Personnel files, including salary records, third party business information submitted in confidence, etc.	Loss of confidence in SAIT's programs, loss of personal or individual privacy
Restricted	Records that are highly sensitive and that could cause extreme damage to SAIT's integrity, image or effective service delivery. They are available only to specific, named individuals (or specific positions).	Restricted areas, credit card numbers, social insurance numbers, personal medical records, budget prior to public release, criminal records/investigations, etc.	Loss of public safety, extreme or serious injury, destruction of partnerships and relationships

D. Non-compliance

1. If questions about access, compliance or use of records arise and cannot be resolved through SAIT's processes or appear to have significant impact on record integrity and processes, matters must be escalated to the CFO and vice president, finance and corporate services for resolution.

2. Failure to comply may result in disciplinary hearings under procedure HR 4.4.1 Corrective Action Procedures.

PROCEDURE

SAIT

POLICY/PROCEDURE REFERENCE

AD.3.2	Records Management policy
AD.3.2.2	Transitory Records procedure
AD.3.2.3	Retention and Disposition Schedule procedure

PROCEDURE