SAIT

AD.3.3.1 DATA GOVERNANCE PROCEDURE	
Section:	Administration (AD)
Subject:	Data Governance
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:	June 6, 2016
Revision:	September 1, 2016 (reformatted)

PROCEDURE

APPROVED: _____

President and CEO

POLICY

The Board of Governors recognizes the importance of data and the information derived from that data. To realize maximum benefit, SAIT will actively manage activities related to the creation, collection, storage, maintenance and sharing of institutional data that is stored electronically, in hard copy, in centrally managed databases or systems, in both academic and administrative offices, and that may exist as structured, unstructured, summarized and aggregated data.

PROCEDURE

DEFINITIONS

Access — The permission rights assigned to allow data custodians to view, copy, enter, download, update or query data.

Aggregated data — Information that is collected and compiled into a summary format, typically for the purposes of reporting or statistical analysis.

Data	Facts, numbers, letters and symbols collected by various means and processed to produce information.
Data integrity	The accuracy and consistency of data over its entire lifecycle.
Data quality	The validity, relevancy and currency of the data.
Data security	The data custodian's access to data and the amount of access each data custodian is allowed.
Data source	The primary location from where data comes. It can be a database, a dataset, a spreadsheet or hard-coded data.
Information	Data elements that have been processed into a meaningful format.
Institutional data	Data created, collected, maintained, transmitted and stored by or for the institution to conduct institution business. It includes data used for planning, managing, operating, controlling or auditing institution functions and operations and as defined by the Data Governance Council/Steering Committee. It is not limited to data or information stored on centrally managed databases/servers. Data can also be stored on hosted services, individual desktops, paper files and electronic files such as spreadsheets.
Structured data	Data that resides in fixed fields within a record, file or data. This includes data in relational databases and spreadsheets.
Summarized data	Data that is combined from different sources and provides an easy-to-read report that identities findings and recommendations.
Unstructured data	Any document, file, image, report, form, etc. that has no defined standard structure.

GOVERNING PRINCIPLES

1. Institutional data is one of SAIT's most important resources. SAIT is the owner of all institutional data and determines how institutional data and information will be shared.

Schools/departments have responsibilities for particular elements and/or aspects of the data.

2. Data will be managed as a business critical resource by following data management best practices and principles that safeguard the data's integrity, security, ownership and access.

3. This procedure does not apply to research data created or used for the purposes of scholarly activity or applied research projects.

4. Every data source must have defined and delegated roles of authority that are responsible for the integrity, security, accuracy and implementation of the data.

5. Wherever possible, data must be collected once, at the source, and made available to data custodians with legitimate business needs.

6. Data must be recorded as accurately and completely as possible by the most informed source, as close to the point of creation as possible, in an electronic format at the earliest opportunity.

7. To uphold the integrity and quality of the data they enter and access, all data custodians must ensure they follow the appropriate procedures.

8. Data must be accessed and used only for its intended purpose. Data must not be accessed or manipulated for personal gain or out of personal interest or curiosity.

9. Data custodians must:

    a) Comply with the *Freedom of Information and Protection of Privacy Act* and SAIT's FIRST principles when accessing data.

    b) Respect the privacy of individuals whose records may be accessed. No subsequent disclosure of personal information contained in files/databases/systems may be made. Disclosure includes but is not limited to verbal references or inferences, correspondence, memoranda or sharing of electronic files.

10. Data must be protected from unauthorized access and modification. In particular:

    a) Appropriate data security measures must be adhered to at all times to ensure the data's integrity, quality and safety.

PROCEDURE

b) Authorization for access to data is not transferrable from the person who has received the authorization to another individual.

c) Data in electronic formats must be protected by appropriate electronic safeguards and/or physical controls that restrict access to only authorized users.

d) Data in hard copy format must be stored in a manner that restricts access to only authorized users.

11. Data must be maintained and managed over time in an auditable and traceable manner.

12. Data must not be duplicated unless absolutely essential and all duplications must have the approval of the appropriate authorities. Wherever possible, SAIT should avoid maintaining redundant and duplicate data in multiple systems.

13. Data definitions and terms must be defined consistently and be accessible across the institution.

14. When retention of data is no longer required for administrative, legal or historical reasons, disposition in accordance with the Classification Scheme and Records Retention Schedule should be applied.

PROCEDURE

A. Scope

1. Data governance will apply to all systems and system components used to conduct SAIT's business. This takes into account SAIT's Enterprise Resource Planning (ERP) system as a way of integrating SAIT's data and processes into a single system with a modular software application. All the modules of SAIT's ERP system (Banner) and systems that exchange data are included.

2. All systems or applications that contain institutional data fall under the Data Governance Steering Committee's governance.

B. Data Management Roles and Responsibilities

1. Data custodians may act in one or more specific roles when creating, collecting, maintaining, transmitting, accessing or using institutional data and must understand and fulfill the responsibilities associated with their roles.

2. SAIT will establish and manage institutional data using the principles of stewardship and data sharing. Roles (and associated responsibilities) have been established to promote and safeguard access to and the integrity and security of institutional data**.** These roles include:

Data custodian	An individual who needs and uses data as a part of that individual's assigned duties. This may include reading, entering, downloading, copying, querying or updating data or information.
Data owner	SAIT is the owner of all institutional data, and determines how institutional data and information will be shared. Schools/departments have responsibilities for particular elements and/or aspects of the data**.**
Data steward	A person within the school/department responsible for all queries and/or issues related to data. A data steward is a business user with expert knowledge of business processes and how data is used within those processes. The data management activities assigned to the data steward may be assigned or delegated by a data trustee. A data steward may be a member of the Data Governance Team.
Data technician	Maintains the technical infrastructure of SAIT systems, implementing access rights and controls to ensure the accuracy, integrity, security and privacy of institutional data. A data technician works with data stewards to ensure data-related issues are escalated to the appropriate governing body in a timely manner. A data technician may be a member of the Data Governance Team.
Data trustee	Accountable for the security, privacy, data definitions, data quality and compliance with data management policies and standards for a specific school/department. Each trustee is responsible for that trustee's assigned data, and for approving requests for access to that assigned data. While data will be transported, matched and eventually stored electronically, this procedure covers the use of shared data at all stages, including but not limited to data used in reports and documents, whether electronic or in print. A data trustee may be a member of the Data Governance Council.

C. Data Governance Structure and Responsibilities

The groups outlined below govern the management of, access to, and accountability for data:

Data Governance Council	The Data Governance Council is SAIT's Executive Management Committee. It sets the overall mission and strategic goal(s) of the data governance effort, and secures the funding, resources and cooperation needed to support that effort. Key is its ability to make decisions regarding data from an "enterprise" perspective.
Data Governance Steering Committee	Chaired by the vice president, finance and corporate services. He or she may delegate or assign any person the authority to chair the committee. It includes data trustees and Information Systems department representatives. The committee develops a task list for the Data Governance Team to resolve problems escalated from lower levels of data management. It reports to the Data Governance Council, which serves as a decision-maker for escalated issues.
Data Governance Team	The Data Governance Team includes data technicians and data stewards. Responsibilities include identifying and applying data governance principles, developing policies and procedures, and ensuring sustainability of institutional data governance. The team's role is to provide recommendations and escalate issues to the Data Governance Steering Committee.

D. Security Classification of Data

1. Data must be assigned a security classification that identifies ownership and control. Data falls into one of the four categories as set out below.

Security Classification	Description	Examples	Risk
Unrestricted	Data and information that is created in the normal course of business that is unlikely to cause harm. Unrestricted data and information is 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	Data and information that is sensitive outside of SAIT and could impact service levels or performance. Authorized access (to employees, contractors, sub-contractors and agents) on a need-to-know basis for business-related purposes.	Grades, data of birth, personal contact information other than SAIT email addresses, etc.	Disruption to business if not available
Confidential	Data and information that is sensitive within SAIT and could cause serious loss of privacy, competitive advantage, loss of confidence in SAIT programs or damage to partnerships, relationships and reputation. Data and information will be available only to a specific function, group or role.	Personnel files, including salary data, third party business information submitted in confidence, etc.	Loss of confidence in SAIT's programs, loss of personal or individual privacy

Restricted	Data and information that is highly sensitive and could cause extreme damage to SAIT's integrity, image or effective service delivery. Information 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

E. Procedures to Support Institutional Data Governance

1. To support and achieve data governance at SAIT, it is necessary to develop effective data management practices and safeguards that comply with all applicable laws, regulations and best practices. This includes effectively documenting the data trail through the implementation of processes associated with accessing, retrieving, reporting, managing and storing data.

2. Additional data management procedures that may be established through the above governance structure include, but are not limited to:

   a) Data Access

      SAIT will establish a set of procedures for requesting permission to access institutional data. Role responsibility will be established to determine access levels and distribution.

   b) Data Classification, Definition and Standards

      SAIT will establish and maintain institutional data classification standards, along with definitions for data and how data is derived and how it is intended to or can be used.

   c) Data Collection and Maintenance

      SAIT will identify and maintain authoritative sources of data, identifying operational responsibilities for data collection and maintenance. This will include establishing governance by participating in due diligence activities associated with institutional data hosted/stored externally offsite.

d) Data Documentation and Metadata

SAIT will document and define guidelines for data elements, establishing a metadata standard that represents data needs across all systems. Documentation for data should include the algorithms and decision rules for derivation. Documentation should contain description of the rules by which the data was constructed, and information about the data structure and the update cycles necessary for the accurate interpretation of the data.

e) Data Management Roles and Accountabilities

SAIT will establish and manage institutional data using principles of stewardship and data sharing. This will include establishing responsibilities to define and classify data. This also includes establishing a governance structure for enabling decisions to be made in a timely manner at the appropriate institutional levels.

f) Data Quality

The quality of data will be actively managed. Standards for data quality, validity, availability, access, definition and use will be established, monitored and enforced to provide the highest quality of data. Role responsibility will be established to create procedures and practices to ensure data quality is maintained in both update and correction situations.

g) Data Security

SAIT will establish and maintain a classification of security access to protect data from inappropriate use. Procedures will be established to ensure data safeguards are established that reflect federal and provincial regulations to protect data from deliberate, unintentional or unauthorized alteration, destruction or inappropriate use or disclosure.

h) Training

SAIT will document and communicate to relevant audiences all applicable information and procedures relating to data by promoting understanding of the appropriate use of data classification, of role responsibilities, and of the impact of decisions made using data. Training material will be periodically reviewed and renewed as required.

i) User Support

SAIT will identify systems housing of institutional data and define the extent of support to data access and interpretation of what is available to data users. Documentation of data resources will be provided to assist data custodians in the interpretation and use of institutional data. An appropriate use policy will be created according to applicable regulations and SAIT policies.

F. Non-compliance

1. If questions about access, compliance or use of data arise and cannot be resolved through SAIT's processes or appear to have significant impact on data integrity and information processes, matters must be escalated to the Data Governance Steering Committee for resolution.

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

POLICY/PROCEDURE REFERENCE

AD.3.3 Data Governance policy