Athabasca University

PROCEDURE

Information and Data Stewardship and Data Custodian Procedure			
Parent Policy	Information and Data Management Policy		
Policy Sponsor	Vice President Information Technology and Chief Information Officer (VPIT & CIO)	**Category**	Administrative
Policy Contact	Chief Information and Security Officer (CISO)	**Effective Date**	December 12, 2019
Procedure Contact	Data Steward for each Business Area Data Custodian Manager (IT)	**Review Date**	December 12, 2024

1. Purpose

Governance of information and data assets in the control of the University requires data stewardship and data custodian responsibilities. This procedure provides stewardship and custodian guidance for the security, integrity, availability and the appropriate security classification levels associated with information and data assets in the control of the University.

2. Scope

This procedure applies to stewardship and custodian responsibilities for all data, content and information, regardless of medium. Applies to all areas of the University who hold responsibility for implementing procedures related to types of data; e.g. Research Data (Research), Systems data such as Learning Engagement Data, Student Records and Operational Data (IT), Privacy and Records Management (Governance), Archives and Learning Resources (Libraries), Personnel Records (HR), Financial Records (Finance).

3. Definitions

Data Custodian	Responsible for the technical environment and database structure necessary to ensure safe custody, transport and, storage of data. Development and implementation of business rules may be done in collaboration with business areas and their data stewards.
Data Sharing	The transfer of data between different organizations, branches or departments to achieve an improvement in the efficiency and effectiveness of public service delivery.

Data Steward	A subject matter expert who is designated by an executive role. This role has operational responsibility for data and information files in the business domain including: the identification of operational and business intelligence data requirements within an assigned subject area; the quality of data and information, business definitions, data integrity rules, compliance with regulatory requirements and conformance to information/data policies and procedures; application of appropriate security and access controls; and identifying and resolving related issues.
Data Stewardship	The business/operation area accountable for the data set. Business areas responsible for data stewardship within the University include: e.g. Research Data (Research), Systems data such as Learning Engagement Data, Student Records and Operational Data (IT), Privacy and Records Management (Governance), Archives and Learning Resources (Libraries), Personnel Records (HR), Financial Records (Finance).
Data Quality	While there is no universal definition for Data Quality, Statistics Canada defines it as the quality of information in terms of its fitness for use. This is a multidimensional concept embracing both the relevance of information to users' needs, and characteristics of the information such as accuracy, timeliness, accessibility, interpretability and coherence that affect how it can be used.
Information and Data Security Classification Levels	Security levels that will be used to classify all data and information that are received, created, held by or retained on behalf of the University. Typical classifications are public and protected (e.g., need to know, confidential and restricted).
Standard Operating Procedure (SOP)	A standard operating procedure addresses process-related information that is below the level of policies and procedures. Their content often inform the Policy Framework. A SOP is highly detailed, regularly revised and is deemed internal to the University, although a SOP may be shared on a need-to-know basis.

4. Guiding Principles

4.1. Business areas within the University are accountable for the privacy, security and protection of data holdings within their area of operation.

4.2. Provide subject-matter expertise regarding the authoritative version of any data they hold.

4.3. Development of best practices and standards will be built collaboratively by IT under the guidance of the Data Custodian Manager reporting to the CISO to ensure standards set for structure, classification, collection, accuracy, consistency, quality, access and retention of data (and associated metadata) are followed by all database administrators in IT.

4.4. Other key responsibilities of data stewardship will be to:

a. Adhere to the University's data governance policies.

b. Determine data required to meet business objectives.

c. Resolve issues related to definition, collection, management and authorized use.

d. Identify content for data quality verification and fitness for use.

e. Define appropriate uses in order to maximize the benefits of the data to the organizations. Promote awareness of the business area's data holdings.

f. Data Sharing within the University. Any external sharing with be governed by relevant procedures and consultation with University Relations

4.5 The Data Custodian(s) role resides in IT and is responsible to interact with the Data Stewards in the following ways:

a. Reference Data – The Data Custodian Manager must have the ability to create and maintain consistent reference data and be the holder of the master data definitions.

b. Publishing – The Data Custodian Manager advises on the publishing and appropriate use of relevant University Community data across the organization, tracking usage/relevance/quality of data sources.

c. Metadata Manager – Each Database Administrator in their responsibility as a Data Custodian works with the Data Custodian Manager to create and manage the metadata for published data sources to ensure its usability and scalability across the enterprise.

d. Reconciliation – Each Database Administrator in their responsibility as a Data Custodian works with the Data Custodian Manager as the last line of defense for data integrity and quality issues across multiple stakeholders and business units.

e. Continuous communication and collaboration with the Data Stewards is essential for the Data Custodian Manager and the Database Administrators in their responsibility as data custodian to keep informed about business changes that impact systems and the data.

f. Once changes have been verified by the Data Custodian Manager, the Database Administrators in their responsibility as data custodian can then ensure the data asset can be scaled across the organization and leveraged appropriately.

g. The Database Administrators in their responsibility as data custodian is the technical partner for the data steward. The two must work as two sides of the same coin.

h. The Data Steward is the “go-to” person within a business domain. Data Stewards must retain responsibility for the data content, quality and integrity.

5. Applicable Legislation and Regulations

Freedom of Information and Protection of Privacy Act
Electronic Transactions Act
European Union General Data Protection Regulation (GDPR)

NOTE: Other legislation relevant to specific business areas may also be applicable.

6. Related Procedures/Documents

Security of Digital Information and Assets Policy and related Procedures

NOTE: The subject matter and scope of this procedure are also supported by internal-use only Standard Operating Procedures, including SOPs unique to AU business areas.

History

Date	*Action*
December 12, 2019	Executive Team (Policy Approved)