Athabasca University

POLICY

| Information and Data Management Policy | | | |
|---|---|---|---|
| **Policy Sponsor** | Vice President Information Technology and Chief Information Officer (VPIT & CIO) | **Category** | Administrative |
| **Policy Contact** | Chief Information Security Officer (CISO) | **Effective Date** | December 12, 2019 |
| **Approved By** | Executive Team | **Review Date** | December 12, 2024 |
| **Approved Date** | December 12, 2019 | | |

## 1. Purpose

Athabasca University is a 100% digital technologies-based post-secondary institution. Within this digital environment, the University Community must be able to trust that their privacy is protected and that their data will not be misused. As such information and data assets must be well-managed to ensure security, integrity, availability and protection. In addition, the University's information and data assets hold strategic value. Together these objectives enable the University Community to achieve its strategies and mandates, improve the quality of decision-making, as well as supporting the delivery of curricula, programs and services.

## 2. Scope

This policy applies to the governance and management of all information and data assets regardless of media. This policy also encompasses digital identity management and classification levels integral to strong Data Governance. The scope of Data Governance responsibilities includes the overall management of the availability, usability, integrity, and security of the University's information and data assets.

This policy does not apply to information conveyed verbally and not recorded.

Athabasca University is in control of both transitory and official information and must manage it throughout its lifecycle. The Chief Security Information Officer is the lead for overall security management of the related technical environments. This responsibility is shared with any business areas within the University who ensure stewardship for various types of digital data (operational, research etc.) they collect or acquire. The University Community shares responsibility for ensuring their information and data use that conforms to the policies and practices prescribed by information and data governance.

## 3. Definitions

| | |
|---|---|
| **Data** | The terms data, information, and knowledge are frequently used for overlapping concepts. The main difference is in the level of abstraction being considered. Data is often the lowest level of abstraction. |
| **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 Governance** | Refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. A sound data governance program includes a governing body, a defined set of procedures, and a plan to execute those procedures. |
| **Data Management** | Comprises all disciplines related to managing data as a valuable resource. |
| **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). |
| **DevSecOps Practices** | Building security into all aspects of the technology lifecycle and its assets into requirements, into design, into code, and into deployment, logging and monitoring.<br>*DevSecOps=Development, Security and Operations* |
| **Identity Management** | The set of policies, procedures and standard operating procedures (SOPs) for ensuring that the proper people in the |

| | |
|---|---|
| | University community have the appropriate access to technology resources. Identity Management systems fall under the overarching umbrella of IT security and Data Management. |
| **Information/Data Asset** | Includes all data, information and intellectual property. |
| **Information Management** | Information management involves the planning, directing and controlling of all of the University's IT assets to meet corporate goals and to deliver programs and services. Information management refers to the application of consistent practices related to planning, creation, capture or collection, organization, use, accessibility, dissemination, storage, protection and disposition (either destruction or permanent retention) of information. |
| **Lifecycle (IT)** | The span of time between the creation of an information/data asset and its disposal. |
| **Protected Information** | Information that is protected as per the Data Classification procedure of the Information and Data Management Policy. |
| **Standard Operating Procedure (SOP)** | A standard operating procedure addresses process-related information that is below the level of policies and procedures. Their content often informs 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. |
| **University Community** | All faculty and staff, students, Board Members, contractors, postdoctoral fellows, volunteers, visitors and other individuals who work, study, conduct research or otherwise carry on business of the University. |

## 4. Guiding Principles

**4.1.** The VPIT & CIO responsible for articulating practices to ensure the security and management of information and data.

a. Effective and efficient management of information and data is a shared responsibility between the VPIT & CIO and data custodians across the University.

b. Information and data management must be integral to the University's DevSecOps Practices.

**4.2.** Identity management must reflect a trust-worthy relationship between the University and its information users.

a. Individual rights and values are upheld by providing choices for service delivery channels, obtaining their informed consent and empowering them to control their own identity to the extent possible

b. Accuracy and integrity of identity-related data is maintained.

**4.3.** Information and data management must be integral to the online architectural vision for the University.

a. As an online university, information and data management should utilize technical storage capabilities and a systems approach that ensure data can be stored, retrieved, archived and removed in a similar fashion for all data custodians.

**4.4.** Information should be clearly identified following a shared data dictionary cross all data custodians.

**4.5.** Information must be stored digitally in the University's secure cloud so that it can be retrieved as part of Disaster Recovery practices within Business Continuity Planning practices.

**4.6.** Information should be created digitally and will be managed digitally, except in these circumstances:

a. Information in paper format should only be used in specific circumstances related to the need for a physical signature.

b. Information in paper format required to retain and retrieve as per FOIP legislation and records management practices should be digitized using AU digitization tools.

**4.7.** As the custodian IT is responsible for ensuring digital information is purged regularly as per the data retention rules and schedules and to ensure legislative compliances are enforced.

**4.8.** Collection, use and disclosure of information and data must comply with legislation, regulations, and contractual requirements.

**4.9.** Protecting the security, integrity and quality of information and data will be paramount. IT staff will develop processes that:

a. Guarantee data custodians can maintain relevance, consistency and accuracy of the data they manage over time and through technological change; and,

b. Ensure data custodians can keep data accurate and reliable for shared access where applicable.

c. Support assignment of appropriate security classification levels for protected information.

**4.10.** Students whose country of residence is under European Union General Data Protection Regulation (GDPR) have the right to request all data related to their interactions with any part of the University and its online offerings in which they partake. In order to fulfill GDPR compliance IT must:

a. Establish a single data record per student to which all of their interactions with any academic or operational part of the University is recorded; exceptions may occur when the student explicitly "opts-in" to participate in as part of a larger research or marketing initiative.

## 5. Applicable Legislation and Regulations

*Electronic Transactions Act*
*Freedom of Information and Protection of Privacy Act (FOIP)*
*Canadian Anti-Spam Legislation (CASL)*
*European Union General Data Protection Regulation (GDPR)*

## 6. Related Procedures/Documents

Code of Conduct for Members of the University Community
Protection of Privacy Policy
Records Management Policy
Digital Governance Framework for AU
Security of Digital Information and Assets Policy and related Procedures
Information and Data Stewardship and Data Custodian Procedure
Information and Data Quality Procedure
Data and Information Security Classification Procedure
Identity Management Procedure

NOTE: The subject matter and scope of this policy and its related procedures are also supported by internal-use only Standard Operating Procedures.

## History

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