Athabasca University

PROCEDURE

Data and Information Security Classification 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	Chief Information Security Officer (CISO)	**Review Date**	December 12, 2024

1. Purpose

This procedure describes the four security classification levels that must be applied to all data and information in the custody and/or under the control of the University. The appropriate application of security classification assesses the integrity, availability, sensitivity and/or value of data and information. Security classifications are utilized to make decisions to disclose information or share data externally as well as inform the online storage specifics related to the data's classification.

2. Scope

The procedure applies to all data and information managed by the University. This procedure aligns with the data and information security classification levels established by the Government of Canada and by the Government of Alberta, and supports data and information sharing across jurisdictions. Any exceptions to an assigned security classification will be made under the authority of the Chief Information Security Officer.

3. Definitions

DevSecOps Practice	Building security into all aspects of the technology lifecycle and its assets into requirements, into design, into code, and into deployment, logging and monitoring. *DevSecOps=Development, Security and Operations*
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).
Sensitive Data and Information	Sensitive data is associated with a person and is typically identifying. Any data or information that reveals: racial or ethnic

	origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; and data concerning health or a natural person's sex life and/or sexual orientation.
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.
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. Four data and information security classification levels that will be used to classify all data and information that are received, created, held by or retained on behalf of the University.

4.2. Security Classification Levels are:

a. PUBLIC – Applies to data and information that, if compromised, will not result in injury to members of the University Community.

   i. Public was formerly known as Unrestricted

   ii. Public information is available to employees and the public

b. PROTECTED A – Applies to data and information that, if compromised, could cause injury to the University Community.

   i. Protected A was formerly known as Protected

   ii. Protected A information is available to employees and stakeholders on a need to know basis.

c. PROTECTED B – Applies to data and information that, if compromised, could cause serious injury to the University Community.

   i. Protected B was formerly known as Confidential

   ii. Protected B information is available only to specific functions, groups or roles

d. PROTECTED C – Applies to data and information that, if compromised, could cause extremely grave injury to the University Community.
   i. Protected C was formerly known as Restricted
   ii. Protected C information is available to specified positions only

4.3. DevSecOps practices are employed to address data and information security in the Athabasca Cloud, including multiple levels of security including, but not limited to, how access to the data is assigned and logged and how data is encrypted both at rest and in transit.

4.4. For all classification levels of data, the following best practices apply:

a. Wherever possible, data should be in digital format. Exceptions would be any data that is required for legislative compliance to have ink signatures (digital signatures not accepted).

b. PROTECTED A, B & C information and data must be managed within a secure environment, and transmitted with digital security measures appropriate for the protection of the information and data (e.g., Sensitive Data) involved.

c. PROTECTED A, B & C information and data must be secured to ensure that only intended recipients are able to access it.

d. Files and folder access will be carefully controlled; ensuring that only authorized personnel may have access to PROTECTED A, B & C information and data within the PROTECTED categories.

e. Destruction of data complies with the University's data records retention schedule.

f. Disposal of any End-User Device complies with IT asset disposal SOPs.

5. Applicable Legislation and Regulations

European Union General Data Protection Regulation (GDPR)

6. Related Procedures/Documents

Project Management Framework for AU
Privacy Protection Policy
Records Management Policy
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.

History

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