Athabasca University

PROCEDURE

Identity Management 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 Security Officer (CISO)	**Effective Date**	December 12, 2019
Procedure Contact	Chief Information Security Officer (CISO)	**Review Date**	December 12, 2024

1. Purpose

This procedure ensures the University utilizes effective identity management practices by setting out the requirements for the verification, protection and use of the identities of individuals who require access to the University's resources.

2. Scope

This policy applies to all information and data assets, regardless of media, and to the University's business processing infrastructure. The Chief Information Security Officer is responsible for implementing processes to provide assurance that only known and trusted individuals are permitted access to sensitive and valuable information resources. Identity management efforts also include the assurance of identity protection and security for all members of the University Community whose identity information is capture by the University's systems.

3. Definitions

Authentication	A means of verifying the identity of an Authorized User, including by two-factor identity verification.
Data Management	Data management is the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets. Activities comprise data policies, data planning, data element standardization, information management control, data synchronization, data sharing, and database development, including practices and projects that acquire, control, protect, deliver and enhance the value of data and information.

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. *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.
Identity Verification (Two-Factor)	Involves user identifying into an Athabasca University system using their login ID and password and then having a second form of authentication for validation (numerical code texted to mobile phone, email to secondary email address, touch ID, facial recognition, etc.) to prevent use of account based on a stolen password.
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).
Log-In Management	The process of recording and storing accesses to accounts for auditing and security management purposes. Also known as logging.
Sensitive Data and Information (Identity)	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.

4. Guiding Principles

4.1. Identity management systems fall under policies associated with Information and Data Security and Data Management.

a. Identify Management experiences are incorporated into DevSecOps Practices.

b. Identity Management requirements will be open, transparent, understandable and promote trust-building across the University Community in regard to its Sensitive Data and Information.

i. Awareness of how and where Sensitive Data and Information will be used by the University in compliance with privacy protection legislation.

ii. Access to Sensitive Data and Information will be secured proportionately to assessed risks.

4.2. Identity Verification

a. Passwords must be routinely changed by the user.

b. Additional use of a second form of authentication when password reset is requested.

c. All owner, administrative or delegate accounts must have logging turned on for auditing and security management purposes.

4.3. Security breach protocols associated with this procedure are subject to IT Security Incident Responses and Cyber Security Reporting procedures.

4.4. Standard Operating Procedures (SOPs) addressing components of identity management including: authentication and access controls; log-in management audits; levels of identity assurance associated with access requirements; and, user account management processes that are followed are not public information and are on a need-to-know basis only as determined by the Chief Information Security Officer and the VPIT & CIO.

5. Applicable Legislation and Regulations

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

6. Related Procedures/Documents

Code of Conduct for Members of the University Community
Protection of Privacy Policy
Security of Digital Information and Assets Policy and related Procedures
Significant Cyber Security Incident Reporting Procedure
CHRO Security Screening

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)