Athabasca University

PROCEDURE

Account Management Procedure

Parent Policy	Security of Digital Information and Assets 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 provides guidance and direction regarding the granting, maintenance and removal of access to the information technology assets of the University. IT Assets must be protected by controls to ensure that only those persons with a legitimate need to access IT Assets have access, and that the level of access is appropriate to each person’s job duties.

2. Scope

This procedure applies to all employees of the University, all contractors and their respective firms doing business with the University, and where applicable, to a third party associated with the University.

3. Definitions

Account	A means for accessing IT Assets that generally consists of an account name (or User ID) and associated Authentication method.
Account Administrator	A designated employee trained in the use of University software systems for the purpose of performing domain account creation, deletion and deactivation.
Asset Owner	University employee or member of Managed Security Services partner personnel to whom the Vice-President IT and CIO or CISO has delegated the authority to grant access to an IT Asset.
Authorized User	A person who has been granted access to an account and whom access has not been rescinded or terminated.

IT Asset or Assets	Digital information and technology assets, which include: • Software (applications, database management, operating systems, licenses, etc.); • End User Devices (portable storage devices, computers, laptops, tablets, smart phones, displays, net stations, etc.); • Digital Information; • Cloud-based or on-premise Servers (multi-user physical or logical computers, etc.); • Networks (cables, circuits, switches, routers, firewalls, etc.); and • Digital Storage Devices and Systems (cloud-based, removable or fixed devices that retain Digital Information, etc.) owned by, under the custody of, or commercially made available to, the University.
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. Creation of Accounts

a. All Accounts must be managed by an Account Administrator.

b. All requests to create an Account must be made via a New Employee/Position Change Request Form owned by Human Resources (HR) and approved by the applicable Asset Owner(s).

c. Accounts for IT Assets for which no Asset Owner is assigned must be approved by the intended Account holder’s Dean or Director using the New Employee/Position Change Request Form.

d. All Accounts creation will be subject to Standard Operating Procedures.

4.2. Authorized User Responsibilities

a. Authorized Users are responsible for all actions made with their User ID.

b. Authorized Users must not disclose credentials to any other entity at any time.

c. Access to the University’s IT Assets must be governed by the ‘Acceptable Use of Information Technology (IT) Assets Procedure’. Unauthorized access is prohibited, and will be subject to disciplinary action up to and including dismissal.

4.3. Access Requests for third party

a. Accounts may be provided to a third party who is associated with the University.

b. Requests for Accounts process is the same as above.

c. Prior to submission, requests must be approved by the Applicable Asset Owner and CISO and include a start date, end date, and reason for access.

d. These Access Requests must be received at the IT Service Desk 10 days prior to the required access date.

e. These accounts will be disabled on the end date specified on the New Employee/Position Change Request Form.

5. Applicable Legislation and Regulations

Freedom of Information and Protection of Privacy Act

6. Related Procedures/Documents

Protection of Privacy Policy
Records Management Policy
Information and Data Management Policy
New Employee/Position Change Request Form
Alberta Association in Higher Education for Information Technology's ITM Control Framework

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)