Information and Communication Technology Account Management Procedure

Policy Sponsor:	Office of Vice-President Information Technology (OVPIT).
Name of Parent Policy:	Security and Protection of Digital Information and Information and Communications Technology Assets Policy
Policy Contact:	Vice-President IT and CIO
Procedure Contact:	Director of IT Operations
Effective Date of Procedures:	July 25, 2016
Review Date:	Annually

Purpose

This procedure provides guidance and direction regarding the granting, maintenance and removal of access to the information and communication technology assets of Athabasca University (the University). ICT Assets must be protected by controls to ensure that only those persons with a legitimate need to access ICT Assets have access and that the level of access is appropriate to each person's job duties.

Definitions

Account:	A means for accessing ICT 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.
Application:	A software program that collects, manipulates, processes, stores, distributes, displays or prints Digital Information.
Archive:	The relocation of Digital Information to a medium for long-term storage when such information does not need to be readily accessible, but may be needed in the future.

Asset Owner:	An employee of the University to whom the Vice-President IT and CIO has delegated the authority to grant access to an ICT Asset. Asset Owners may delegate their authority to one or more employees of the University.
Authentication:	A means of verifying the identity of an Authorized User.
Authorized User:	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this procedure or this procedure's parent policy.
Backup:	The copying of Digital Information from one electronic medium to another.
Backup Copy:	The copy of Digital Information made during Backup.
Confidential Digital Information:	Information identified as confidential by the person to whom the responsibility for such designation has been delegated by the University.
Digital Information:	Information stored in ICT Assets using binary encoding.
Digital Storage Device:	A device that can retain binary encoded information in a permanent state.
Email Account:	An Account used to send or receive email.
FOIP:	*Alberta Freedom of Information and Protection of Privacy Act.*
Foreign Device:	Any End User Device that has not been issued or provided by Athabasca University or that has not been approved for use by the University's Director of IT Operations.
General Service Account:	A shared Account that is used for communication or information exchange between applications under Software control.
General Service Account Owner:	A person who has been designated as having responsibility for the use of a General Service Account by the Vice-President IT and CIO or the Director of IT Operations.
ICT:	Information and communication technology.

ICT Assets or **Assets:**

Information Communication and Technology Assets, which include:

- **Software** (applications, database management, operating systems);
- **End User Devices** (portable storage devices, computers, laptops, tablets, smart phones, displays, net stations);
- Digital Information;
- **Servers** (multi-user physical or logical computers);
- **Networks** (cables, circuits, switches, routers, firewalls); and
- **Digital Storage Devices and Systems** (removable or fixed devices that retain Digital Information)

owned by, under the custody of, or commercially made available to, the University.

ICT Incident or **Incident:**

Any failure or malfunction of ICT Assets that results in a loss of Service to the University community.

ICT Security Incident:

Any event that has compromised, is suspected of having compromised, or is likely to compromise the confidentiality, integrity or availability of Athabasca University's ICT Assets. Examples include, but are not limited to:

- Computer viruses or malware;
- Loss of laptops, tablets or smart phones containing Confidential Digital Information or Protected Information;
- Unauthorized access to ICT Assets;
- Denial of online service attack; and
- Criminal activities involving ICT Assets.

An equipment or software performance issue, failure or malfunction is NOT considered an ICT Security Incident if there is no indication that it was caused intentionally.

Incident Manager:

An individual designated to assign personnel to, coordinate the response to, and issue a report regarding, an ICT Security Incident or ICT Incident.

ITS:

Information Technology Services department of the University.

Life Cycle:

The span of time between the creation of an ICT Asset and its disposal.

Open Access Asset:

An ICT Asset that can be accessed without the need for prior approval from the Asset Owner.

Privileged Account:	An Account that provides an Authorized User with the ability to control the access or permissions of other Authorized Users.
Protected Information:	Information that is protected under some legislation.
Recovery:	The restoration of point-in-time copies of Digital Information from a Backup Copy.
Responder:	A person assigned by an Incident Manager to investigate an ICT Security Incident or ICT Incident.
Service:	An integrated group of ICT Assets that provides value to Authorized Users.
Security Incident Report:	A written report using the approved ICT Security Incident Report Form.
System Administrator:	A University employee who is responsible for the upkeep, configuration, and reliable operation of ICT Assets.
User ID:	A unique identifier assigned to an Authorized User or Service to enable access to ICT Assets.
VPIT and CIO:	Vice-President Information Technology and Chief Information Officer of the University.

Procedure

1.0 General

1.1 Creation of Accounts

1.1.1 All Accounts must be created in AUME, OPENLDAP, and active directory by an Account Administrator.

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

1.1.3 Accounts for ICT 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.

1.1.4 All Accounts (except Email Accounts) will be created using the format defined within the current Directive on Account Names as maintained by the Director of IT Operations.

1.1.5 All Email Accounts will be created using the following format: firstname.lastname@athabascau.ca.
In the event the *firstname.lastname* combination already exists, the user's middle initial will be used and concatenated to the first name. For example, johnb.smith@athabascau.ca. Should the combination already exist or, if the user does not have a middle name, an additional character will be added to the first name initial combination, starting with the letter z and working backwards to the letter a. For example, johnbz.smith@athabascau.ca.

1.2 Management of Accounts for status changes

1.2.1 The status of an Authorized User changes when there is a change of position or continuing role of an Authorized User.

1.2.2 Notification of a change in status will be communicated using the New Employee/Position Change Request Form.

1.2.3 Human Resources will notify the ITS help desk of an employee's change of status relative to the University at least five days prior to the date of the status change.

1.2.4 Managers, Directors and Deans are responsible for ensuring the ITS help desk is notified of the change in status of a non-employee Authorized User under their direction (e.g. visitor or contractor) at least five days prior to the date of the status change.

1.2.5 Previously held Account access rights of the Authorized User other than the email and assigned NAS storage will be disabled by the help desk on the date and at the time specified on the New Employee/Position Change Request Form or according to other appropriate direction provided.

1.2.6 If the date for disabling an access rights is other than the date of the change in status of the Authorized User, the reason for the extension must be provided on the New Employee/Position Change Request Form. All extensions must be approved by the applicable Director or Dean and by the Director of IT Operations or designate.

1.2.7 In some instances it may be appropriate to transfer Digital Information in the Authorized User's email or personal NAS storage to another Authorized User. The immediate supervisor or Director/Dean of the Authorized User whose position or role is changing may request such a transfer using the New Employee/Position Change Request Form.

1.3 Deletion of Accounts for departing Authorized Users.

1.3.1 A cessation of employment, contract expiry or termination or completion of other relationship with the University of an Authorized User is deemed a departure of the Authorized User.

1.3.2 Notification of a departure event will be communicated using the New Employee/Position Change Request Form.

1.3.3 Human Resources will notify the ITS help desk of an employee departure at least five days prior to the date of the departure.

1.3.4 Managers, Directors and Deans are responsible for ensuring the ITS help desk is notified of a departure of an Authorized User under their direction (e.g. visitor or contractor) at least five days prior to the date of departure.

1.3.5 All Authorized User Accounts and access rights will be disabled by the help desk on the date and at the time specified on the New Employee/Position Change Request Form or according to other appropriate direction provided.

1.3.6 Digital Information in email and assigned NAS storage may at the discretion of the immediate supervisor be made available to other Authorized Users as designated on the New Employee/Position Change Request Form

1.3.7 If the date for disabling an Account is other than the date of the conclusion of the Authorized User's relationship with the University, the reason for the extension must be provided on the New Employee/Position Change Request Form or, for non-employees, in an email from the relevant Director or Dean. All extensions must be approved by the applicable Director or Dean and by the Director of IT Operations or designate.

2.0 Account Review Process

2.1 The ITS help desk will provide a semi-annual report to all ICT Asset Owners that lists all Authorized Users of the ICT Assets for which that ICT Asset Owner is responsible. This report will be reviewed by the ICT Asset Owner, who will, if applicable, confirm to the ITS Help Desk within 30 days of receipt, each Authorized User's continued access.

2.2 The ITS help desk will provide a monthly report listing all network Accounts that have exceeded 30 days of inactivity to the immediate supervisors of inactive Account holders. These reports will help identify Accounts that are no longer used or needed. Any changes in Account status must be communicated, by the Account holder's supervisor, to the ITS help desk within 15 days of receipt of the monthly report.

2.3 Network Accounts not used for 60 days will be disabled and may be reactivated only by submission of a New Employee/Position Change Request Form approved by the Account holder's immediate supervisor.

2.4 The Manager of IT Services and Support will advise the immediate supervisor of Authorized Users of Accounts that have been inactive for more than 6, 12 or 18 months that the Account will be deleted and that any data related to the Account will be provided to the immediate supervisor in digital form. The immediate supervisor may request that the Account not be deleted by responding within 15 days.

2.5 Accounts that have not been accessed for 24 months will be deleted and any data related to the Account provided to the immediate supervisor of the Account's Authorized User in digital form.

3.0 Account Password Management and Lockout

3.1 Account lockout will occur after ten failed login attempts within 15 minutes. Authorized Users of such Accounts will be required to contact the ITS help desk to reset their Account passwords.

3.2 Authorized Users will receive automated email notifications 30 days prior to their Account password expiry date with instructions for updating.

4.0 Password Standards

4.1 Passwords must contain a minimum of eight characters
.

4.2 Passwords must contain at least one number and upper-case letter.

4.3 Passwords will automatically expire and must be changed every 180 days. Expired passwords cannot be reused within the same 365-day period.

4.4 Passwords cannot contain any portion of the Authorized User's name, nickname, relative's names, or birth date.

4.5 Passwords should not be dictionary words or common acronyms.

4.6 Passwords should be unique and not used on other systems or services.

4.7 Passwords must not be publically displayed or exposed to anyone.

4.8 If the security of a password is in doubt, it should be changed immediately.

5.0 Authorized User Responsibilities

5.1 Authorized Users are responsible for all transactions made with their User ID.

5.2 Authorized Users shall not disclose passwords to others at any time.

6.0 Access requests for persons other than employees or contractors.

6.1 Accounts may be provided to persons who are associated with the University but are not employees or contractors of the University.

6.2 Requests for Accounts for associated persons must be made by a Dean or Director using a New Employee/Position Change Request Form and received at the ITS help desk 10 days prior to the required access date.

6.3 Requests must be approved by the Applicable Asset Owner and Director of IT Operations or designate and include a start date, end date, and reason for access.

6.4 Accounts for associated persons will be disabled on the end date specified on the New Employee/Position Change Request Form.

Applicable Legislation and Regulations

None

Related References, Policies, Procedures and Forms

Directive on Account Names
New Employee/Position Change Request Form
Security and Protection of Digital Information and Information and Communications Technology Assets Policy
Protection of Privacy Policy
Records Management Policy

History

Executive Group, July 25, 2016 (associated policy approved)