Disposal of Information and Communication Assets 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:	June 10, 2016
Review Date:	Annually

Purpose

The purpose of this procedure is to provide direction regarding the decommissioning and secure disposal of Athabasca University (the University) ICT Assets and ensure that disposal prevents the release or loss of information.

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Authorized User	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this procedure or this procedure's parent policy.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	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. The Director of IT Operations is responsible for the disposal of ICT Assets by:

    1.1 Confirming ICT Asset(s) ownership and appropriate approvals for disposal.

    1.2 Adhering to the University's Records Management Policy.

    1.3 Confirming information contained on the ICT Asset is not subject to any known grievance, legal claims, complaints, litigation discoveries or requests for information under FOIP.

    1.4 Ensuring implementation of controls to prevent unauthorized release of information through sale or disposal.

    1.5 Securely storing ICT Assets until disposal.

    1.6 Notifying the Finance department of the serial number and date of disposal of any ICT Asset deemed by the Finance department to be a capital asset.

2. Any ICT Asset being considered for resale or donation that contains a Digital Storage Device must be processed using the following procedures. Any ICT Asset that cannot meet these requirements may not be sold or donated.

   2.1 All Software licensed to the University must be deleted.

   2.2 The relevant serial number, asset tag and End User must be documented.

   2.3 The Digital Information on the Digital Storage Device must be rendered unreadable either by:

   - A commercially proven and certified data erasure solution which meets the international erasure standard: US Department of Defense Sanitizing (DOD 5220.22-M, DOD 5220.22-M ECE) and can generate a Certificate of Destruction or Erase Audit Report, or:

   - Encryption of the stored Digital Information and subsequent erasure with a single pass overwrite solution, or:

   - Deletion of the encryption key and erasure with a single pass overwrite solution for a Digital Storage Device that was encrypted.

   2.4 An attestation of the steps that were satisfactorily completed must be prepared.

3. Any Digital Storage Device that cannot meet the minimum erasure requirements as stated in 2.3 must be physically damaged to an extent sufficient to preclude its further use. Such damage will be caused by combustion, crushing, or perforation by Vice-President IT and CIO staff or an agency or contractor specially equipped and certified for the destruction of Digital Storage Devices.

4. ICT Assets that are not donated or sold must be disposed of to an organization that recycles or recovers materials or components of such equipment in an environmentally responsible manner.

Applicable Legislation and Regulations

Alberta *Electronic Transaction Act*
Alberta *Freedom of Information and Protection of Privacy Act*
Copyright Act (Canada)
Criminal Code (Canada)

Related References, Policies, Procedures and Forms

Security and Protection of Digital Information and Information and Communications Technology Assets Policy
Protection of Privacy Policy
Records Management Policy

History

The Board of Governors Athabasca University, June 10, 2016, Motion # 211-08(associated policy approved)