Athabasca University

**PROCEDURE**

| Disposal of Information Technology Assets 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** | |
| **Procedure Contact** | Deputy CIO | **Review Date** | |

## 1. Purpose

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

## 2. Scope

The scope of the procedure is all End-User Devices and on-premise IT equipment owned or leased by the University for its employees and students.

## 3. Definitions

| | |
|---|---|
| **Digital Information or Content** | Binary encoded information. |
| **Digital Storage Device** | A device that can retain binary encoded information in a permanent |
| **End User Device** | A computing device used by End-Users including desktop computers, net stations, laptops, and mobile devices (e.g., tablets, smart phones), monitors headphones and webcams. |
| **FOIP Act** | *Alberta Freedom of Information and Protection of Privacy Act* R.S.A. 2000, c. F-25, as amended from time to time. |
| **IT Assets 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.** Managing Disposal

a. The disposal process for IT Assets will ensure all Digital Information is removed prior to disposal.

b. The Deputy CIO is responsible for managing the disposal of IT Assets, including End-User Devices owned by the University, by:

i. Confirming IT Asset(s) ownership and appropriate approvals for disposal.

ii. Adhering to the University’s Records Management Policy.

iii. In collaboration with the Privacy Office, confirming information contained on the IT Asset is not subject to any known grievance, legal claims, complaints, litigation discoveries or requests for information under the FOIP Act.

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

v. Securely storing IT Assets until disposal.

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

### **4.2.** Resale or Donation

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

b. All Software licensed to the University must be deleted.

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

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

   i. A commercially proven and certified data erasure solution which meets the currently applicable international erasure standard: US Department of Defense Sanitizing and can generate a Certificate of Destruction or Erase Audit Report, or;

   ii. Encryption of the stored Digital Information and subsequent erasure with a single pass overwrite solution, or;

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

e. An attestation of the steps that were satisfactorily completed must be prepared and stored for audit review purposes.

### **4.3.** Elimination

a. Any Digital Storage Device that cannot meet the minimum erasure requirements as stated in 4.2(d) must be physically damaged to an extent sufficient to preclude its further use. Destruction will be performed by an agency or contractor specially equipped and certified for the destruction of Digital Storage Devices.

b. IT 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.

## 5. Applicable Legislation and Regulations

*Alberta Electronic Transaction Act*
*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
Records Management Policy
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) |