Inventory Management Policy (ISP-05)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all IT, Finance and Procurement staff and contractors.

Table of Contents

Introduction

The cornerstone of effective IT security is a knowledge of what systems and services are in use across the University. Such an inventory enables the IT and IT security team to implement controls and manage risks to the University.

Objective

The Objective of this policy is to define the requirements for the creation and maintenance of an inventory of devices, software, and services in use as part of the IT eco system.

Policy Statement

General

A single or federated asset registry is to be created and maintained for all IT devices, services, and software. A device is defined as any item that incorporates computing, memory, and storage. The IT director may choose to extend this to include attractive and valuable items such as large displays and desktop screens.

The asset register is to enable the following:

1. Track the lifecycle of the asset from purchase to deployment, to retirement, to disposal
2. Include critical identifying information including serial number, license keys, description
3. Financial information including purchase price and date for capital items.
4. Internal owner or responsible department
5. Additional other information may be included such as version or release levels

Tagging

Tagging of assets is to be achieved as following

6. Physical assets are to be marked with an ECU Property Tag
7. Logical (Software) services and resources are to be labeled with a software Tag including the business owner of the service.

Responsibilities

8. The CIO, CISO or Qualified Individual is accountable for the execution of this policy and maintenance of the asset register.
9. The IT Director is responsible for maintaining the IT device, software and service asset registry and a process for keeping it up to date and current.
10. Finance and Procurement staff are responsible for notifying the IT director or representative on the procurement, commissioning and decommissioning of both physical and logical assets.