University of Colorado
Colorado Springs

UCCS CAMPUS PROCEDURE

Procedure Title: IT Asset Management Guidelines

Related Policy: 700-002

Functional Area:	Office of Information Technology
Effective:	March 31, 2025
Procedure Primary Contact:	Harper Johnson, AVC IT and CIO
	Xochil Herrera, AVC Accounting and Controller

I. Purpose

A. To enhance control over high-risk, non-capital IT assets (valued under $5,000), also referred to as controlled IT assets. The steps outlined in this procedure aim to reduce the risk of loss, theft, or compromise sensitive data.

II. Scope

A. These guidelines apply to all controlled IT assets, that are owned, used or otherwise operated by the University, regardless of the source of funding, location or intended purpose. The department should track assets that they determine vulnerable to theft, loss, or misuse. Assets valued over $5,000 are tracked by the Office of the Controller and are not covered under these guidelines

III. Definitions

A. Controlled Assets: Non-capital assets (valued under $5,000) that require safeguarding, include: laptops, desktops, tablets. Other assets identified as high risk by the department should also be tracked.

IV. Procedure

A. IT Asset Procurement

1. Purchases should be made through CU Marketplace
   a. CU Marketplace is the University’s preferred electronic purchasing and payment system. It offers online shopping through specific supplier catalogs and processing forms for suppliers without catalogs.
   b. Using the CU Marketplace ensures that your IT purchases are screened for system compatibility and security compliance prior to purchase.

2. Procurement Cards and personal reimbursements are not recommended for purchasing IT assets, exceptions are subject to CU procurement and purchasing policies.
    a. Review checklist for IT purchases and ensure the purchase is reviewed for legal, security, and compliance concerns.
    b. For more information on procurement methods, visit the CU Procurement website.

B. IT Asset Tracking

1. Asset Management Software
    a. All controlled IT assets are tracked using Snipe-IT, an asset tracking software.
    b. Each department will use the asset serial number to identify the asset.
    c. Departments will assign assets to users and report any changes in user status through Snipe-IT.

C. Initial Asset capture

1. Each IT asset has a unique ID or is assigned an asset tag by OIT. This ID is recorded in Snipe-IT and physically affixed to the asset.
2. To tag new or untagged assets, please schedule an appointment with OIT. If you cannot schedule an appointment, contact OIT to have an asset tag mailed to you.

D. IT Asset Inventory/Audit

1. Each school or department must conduct an annual inventory of their assets to ensure that the physical count matches what is recorded in Snipe-IT and that the designated users are correct.
2. Audit results should be updated in Snipe-IT.
3. Audits should take place annually by 6/30.

E. Federal/Government Owned IT Assets

1. Typically, federally purchased equipment becomes the property of UCCS once the grant has ended, unless the equipment is considered Federally/Government Owned which is identified in the terms and conditions of the award. Reach out to your Sponsored Project Accountant for clarification on your federally purchased equipment.

2. UCCS Property Accounting Guidelines and Federal Policies (CFR 200 FAR Part 45, FAR Part 52.245.1, and DFAR Part 245) require that all Federal property be tagged and recorded with records made available for review by the Government.

3. Departmental Asset Managers are designated as Federally owned property custodians by their academic or administrative units with the following responsibilities
    a. Ensure that all Federally owned property bears a property control identification tag issued by the Office of the Controller.
    b. Ensure that all new acquisitions, changes, transfers, and disposals of Federal property are handled and reported in accordance with established procedures and Federal regulations

F. Sensitive Data Management

1. Before transferring an IT asset between users, it must be taken to OIT to be reimaged with a clean hard drive. No device may be transferred between individuals without a clean image.

G. Disposals

1. Refer to UCCS Policy 700-006 Computer and Electronic Disposal.

H. Reporting Lost or Stolen Assets

1. Asset managers should immediately report any lost or stolen IT assets to the Office of Information Technology. After consultation with the OIT, additional reporting to law enforcement or risk management may be deemed appropriate.

V. Roles and Responsibilities

A. Office of Information Technology (OIT):

2. Manages tagging of any controlled asset that does not have its own serial number.
3. All new IT purchases are brought to IT for capture of the unique serial number or tagging.
4. Maintains the consolidated asset list for the campus.
5. Responsible for training new users on how to use Snipe-IT.

B. Office of the Controller:

1. Provides training on procurement and capital asset tracking.
2. Track any IT purchases over capital threshold.

C. Individual Schools/Departments:

1. Responsible for controlled asset management within their areas.
2. Must appoint an asset manager who will oversee and track the controlled assets for their area. The default asset manager will be the Departmental Financial Administrator unless another position is named by the department.

D. Departmental Financial Administrators:

1. Supports departmental procurements, ensuring IT asset purchases comply with CU procurement policies and procedures.
2. Should perform a risk assessment to identify the assets of their department that are considered high-risk and are therefore most vulnerable to theft, loss or misuse.

E. Departmental Asset Managers:

1. Responsible for overseeing each school or department’s controlled asset list.
2. Responsible for ensuring that all IT assets for their area are tagged and added to Snipe-IT with sufficient detail. Asset listing should include an asset name, model, manufacturer, serial number, purchase date, designation as federally owned or not, location and the individual it is assigned to.
3. Update the asset listing in Snipe IT as changes occur in either user or asset information.
4. Responsible for conducting annual asset inventory/audit.
5. Review purchasing data to ensure that all of the department’s controlled IT assets are recorded in Snipe-IT.
6. Must ensure asset disposals comply with UCCS 700-006.
7. Must report lost or stolen assets to OIT and record in Snipe-IT.

VI. Related Resources

A. Snipe IT Asset Management (ITAM) - Help Desk Knowledge Base - University of Colorado Colorado Springs
B. CU Procurement Service Center IT Procurement
C. Appendix A: Asset Risk Assessment

VII. Appendix A: Asset Risk Assessment

Consider using the following methodology when you perform a risk assessment over your department's assets. You may adapt it to meet your needs.

Step 1: Identify all noncapitalized assets by asset type. For example:

- Computers, laptops, tablets, notebooks, monitors, shop tools, shop equipment, power tools, radios, smart phones, cameras, law enforcement weapons, safety equipment, televisions, audio-visual equipment, GPS devices, microscopes, medical devices and optical devices such as binoculars and telescopes.

Step 2: For each asset type identified in step 1, identify risks using the following questions:

a. Is this a new asset type for your department?
b. Would the public expect you to have strong safeguards over this asset type?
c. Is the asset type susceptible to theft or resale?
d. Is the asset type easily converted to personal use?
e. Is the asset type expensive?
f. Is the asset type likely to go unnoticed as missing or broken (such as if infrequently used)?
g. Have you experienced past problems with missing or damaged assets of this type?
h. Is the asset type dangerous and does it present a safety risk to the public?
i. Could the loss of a certain asset type expose you to business risks (such as a data breach, lawsuit, accident, safety issue or reputational harm)?
j. Did you purchase any assets using federal funds? If so, does the awarding agency or Uniform Guidance require you to follow certain requirements?
k. Did you acquire any assets through a federal surplus program? If so, do you have special requirements for asset tracking?
l. Did you purchase any of this asset type using other grant funds that may have special requirements?

Step 3: For each identified risk, determine the likelihood it will occur and how much it could impact the organization. This analysis can help you allocate limited resources to the riskiest assets.

For example, consider these hypothetical situations:

Risk: Desktop computers store sensitive information

- Likelihood of loss: Low because computers are stationary, the building is secured with an alarm, the employees use the desktops daily and their supervisors observe them.
- Potential impact: Very high because employees store significant amounts of confidential information on the hard drives and a data breach would be costly.

Risk: Specialized equipment is susceptible to resale

- Likelihood of loss: Low because equipment is stored in a secured area and one employee checks out the equipment to other employees.
- Potential impact: Moderate because some of the specialized equipment is costly.

Step 4: Develop and implement safeguards based on the risk analysis. You might track and inventory certain categories of assets beyond the required controlled IT assets and exclude others depending on the overall risk. You could also implement special controls to reduce the risk, such as using secured storage or checkout logs.

Step 5: Set a recurring date for subsequent risk assessment reviews. You should perform risk assessments periodically or as circumstances change. For example, it is a best practice to update your department policy every three years and reevaluate your risk assessment at that time.

Step 6: Monitor the effectiveness of adopted safeguards. Make adjustments as needed.