Asset Inventory Guidance

Departments without an IT asset inventory

What is an information technology (IT) asset inventory?

An IT asset inventory is a list of all computing and networking related devices owned, managed, or otherwise used by a department. These devices include computers (desktops, notebooks, servers), network devices (switches, routers, etc), printers, appliances (network attached storage, network capable cameras, etc). The list should contain the same pieces of information for each item, suggested information is listed below.

Why is an IT asset inventory important?

There are a number of reasons that maintaining an inventory of IT assets is important and useful.

- Provides a record of valuable assets for accounting/tracking purposes
- Helps identify areas of potential risk (notebooks storing private data, servers with expired warranties, etc)
- Important piece of information for business continuity planning
- Provides information useful during technical support or in the event of loss/theft (make, model, serial number)

What does our department need to do?

Departments are responsible for developing and maintaining current inventories of their IT assets (computers, network devices, printers, etc), including information about the criticality of the asset and any sensitive data stored on it. A description of asset criticality and information sensitivity is available at http://www.colorado.edu/its/security/assetinventory

Departments are also responsible for providing a copy of the inventory to the campus IT Security Office. For more information, contact security@colorado.edu

These two responsibilities are described in the University Administrative Policy Statements: IT Security in University Operations, Continuity, and Contracting and Information Classification

What information should be gathered?

The amount of information gathered depends on your goals and available resources. To facilitate IT asset inventories, ITS provides two different inventory spreadsheet templates, one listing a minimum amount of information to gather and one listing a larger amount of useful information that can be gathered.

At a minimum, departments should know:

- what IT assets they own (make and model)
- where they are located or a primary location for mobile devices (building and room)
- who is responsible for the asset
- how essential/critical the asset is to the department's business
- what private information is stored on the asset, if any

ITS encourages departments to collect information in addition to these minimum items and provides a more complete spreadsheet template giving examples of other useful pieces of information including: serial number, B-jack number, CU property tag number, etc.

What should we do with the information?

IT asset inventories should be stored in a secure manner, since they indicate which items are essential or store sensitive information. A copy should be provided to the IT Security Office, who will store it securely. The IT Security Office should receive at least the information described in the basic sample spreadsheet for all systems storing private data. This information should be updated at least once a year or whenever a major change occurs (i.e. private data handling is moved to a different system). Contact the IT Security Office for details on securely transferring the information.

The information can be used for other planning and accounting purposes. Identifying critical assets is an important piece of business continuity planning as well as performing IT risk assessments. The inventory can also be very useful when performing technical support or reacting to a theft/loss. In both situations, having easy access to serial numbers or property tag numbers can streamline the process.