



IT Asset Control & Disposal Policy Guide June, 2009

Often times, Cascade customers would like to develop an internal process or procedure for controlling and managing the disposal of IT assets. This is helpful in creating standards for the organization and for training staff in implementing this procedure.

Below is a generic policy for IT asset control and disposal. Based on current priorities, this policy emphasizes the need to control data on IT equipment during use, internal transfer and disposal. It is important for an asset disposal policy to be tied to an IT asset usage policy because many of the issues faced in disposal should be considered and communicated to employees when they are given assets to use. A policy like this touches many aspects of an organization and should be developed and coordinated with a company's Purchasing/Procurement, Information Technology, Environmental/Risk Management, and Facilities departments.

Cascade also produced a tool titled "IT Asset Retirement Project Development Considerations," which helps organization identify their asset management and retirement needs and to develop an entire program around these needs. Please contact us if you need a copy of this document.

You can also search the web with the keywords "Asset Disposal Procedure" to find a large number of published disposal guides, typically written for government and educational institutions.

Sample IT Asset Control and Disposal Policy

- Taken from the Computer Technology Documentation Project

1.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for an asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

2.0 Purpose

This policy is designed to protect the organizational resources on the network by establishing a policy and



procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.

3.0 Assets Tracked

This section defines what IT assets should be tracked and to what extent they should be tracked.

3.1 IT Asset Types

This section categorized the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Printers, Copiers, FAX machines, multifunction machines
4. Handheld devices
5. Scanners
6. Servers
7. Firewalls
8. Routers
9. Switches
10. Memory devices

3.2 Assets Tracked

Assets which cost less than \$100 shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

1. Hard Drives
2. Temporary storage drives
3. Tapes with data stored on them including system backup data.
4. Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes.

3.3 Small Memory Devices

Small memory storage assets will not be tracked by location but by trustee. These assets include:

1. Floppy disks
2. CD ROM disks
3. Memory sticks

If these types of devices are permitted for some employees, the trustee of the device must sign for receipt of these devices in their possession. All employees must also agree to handle memory sticks, floppy disks, and CD ROM disks in a responsible manner and follow these guidelines:

1. Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
2. Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network should be on the IT department list of approved programs.

The Memory Device Trustee agreement allows employees to sign for receipt of these devices and agree to handle these devices in accordance with the terms of this policy. This form must be submitted by all employees that will work with any organizational data when the employee begins working for the



organization. It will also be submitted when employee receives one or more memory sticks, temporary storage drives, or data backup drives.

4.0 Asset Tracking Requirements

1. All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.
2. An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.
3. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

5.0 Transfer Procedure:

1. Asset Transfer Checklist - When an asset type listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Checklist must be filled out by the trustee of the item and approved by an authorized representative of the organization. The trustee is the person whose care the item is in. If the item is a workstation, then the trustee is the most common user of the workstation. For other equipment, the trustee is the primary person responsible for maintenance or supervision of the equipment.

The trustee must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new trustee, or being disposed of. The following information must be filled in:

1. Asset Type
2. ID number
3. Asset Name
4. Current Location
5. Designated Trustee
6. New Location
7. New Trustee
8. Locations of Sensitive Data

Once the trustee fills out and signs the Asset Transfer Checklist form an authorized representative must sign it.

2. Data entry - After the Asset Transfer Checklist is completed, it will be given to the asset tracking database manager. The asset tracking database manager will ensure that the information from the forms is entered into the asset tracking database within one week.
3. Checking the database - Managers who manage projects that affected equipment location should check periodically to see if the assets that recently were moved were added to the database. The database should provide a recent move list which can be easily checked. Managers should check the database weekly to be sure assets moved within the last 2 or 3 weeks are included in the database.

6.0 Asset Transfers

This policy applies to any asset transfers including the following:

1. Asset purchase



2. Asset relocation
3. Change of asset trustee including when an employee leaves or is replaced.
4. Asset disposal

In all these cases the asset transfer checklist must be completed.

7.0 Asset Disposal

Asset disposal is a special case since the asset must have any sensitive data removed during or prior to disposal. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
2. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
3. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved technologies are to specified in a Media Data Removal Procedure document by asset type including:
 1. Floppy disk
 2. Memory stick
 3. CD ROM disk
 4. Storage tape
 5. Hard drive.
 6. RAM memory
 7. ROM memory or ROM memory devices.

8.0 Media Use

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

1. Floppy disk
2. Memory stick
3. CD ROM disk
4. Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data assessment process.

1. Unclassified - Data may be removed with approval of the first level manager and the permission is perpetual for the employee duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
2. Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
3. Confidential - The data may only be removed from secure areas with permission of a Vice - president or higher level of management. There must be some security precautions documented for both the transport method and at the destination.



4. Secret - - The data may only be removed from secure areas with the permission of the President or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
5. Top secret - The data may never be removed from secure areas.

9.0 Enforcement

Since data security and integrity along with resource protection is critical to the operation of the organization, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.