IT Asset Control & Disposal Policy Guide

January, 2017

The following is a generic framework policy for IT asset control and disposal. This framework emphasizes the need to control data on IT equipment throughout its use, internal transfer, and disposal. It is important that an asset disposal policy to be tied to an IT asset usage policy as they involve many of the same issues. This policy impacts many different aspects of the organization and should be developed and coordinated with stakeholders within the Purchasing/Procurement, Information Technology, Environmental/Risk Management, and Facilities Management departments.

This document is intended as a policy framework and not a set of procedures that inform your organization on how to meet policy requirements. You should create your policy first and then develop the procedures and processes that derive from it.

Available resources include the following:

- NIST Special Publication 800-88, Revision 1: "Guidelines for Media Sanitization" *(https://www.nist.gov/node/561096)* – this is the definitive guide for determining the organization's tolerance for risk and establishing appropriate methods and systems to sanitize data on storage devices.

- HIPAA Security Rule Guidance Materials *(http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html)* – The U.S. Department of Health and Human Services has compiled a number of resource materials to help establish security standards and procedures that are helpful for the healthcare industry and anyone else handling confidential information.

- PCI – DSS Sample Policy Template *(http://www.pcidssguru.com/policy/a-sample-policy-for-pci-dss/)* – this template provides a good overview of the elements of an organizational policy that meets the payment card industry standard.

Be sure to speak with a representative from Iron Mountain if you would like further assistance. We can provide training, tools, and examples of best practices in order to get you started and further improve your programs & procedures.

Sample IT Asset Control and Disposal Policy

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 will also protect any data being stored on those assets. This asset policy also covers the disposal of IT 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 is to maintain data security. 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 location to another. This policy will provide for an asset tracking database to be updated so that the location of all computer equipment is known at all times. This policy will help network administrators protect the network by enabling them to know what user and computer is at what station in the event of a network intrusion. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted while in transit.

2.0 Purpose & Responsibility

This policy is designed to protect the organizational resources on the network by establishing policies and procedures for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of a data breach or loss due to poor planning.

The Security Officer [insert role] is ultimately responsible for the development, implementation and enforcement of this policy.

3.0 Assets Tracked

Defines which IT assets should be tracked and to what extent.

3.1 IT Asset Types

Categorized the types of assets subject to tracking – including:

1. Desktop workstations
2. Laptop mobile computers
3. Mobile phones and tablets
4. Printers, Copiers, Fax machines, multi-function machines
5. Handheld devices
6. Scanners
7. Servers
8. Firewalls
9. Routers
10. Switches
11. Memory devices

3.2 Assets Tracked

Assets that cost less than $ [INSERT AMOUNT] and do not contain date should not be specifically tracked. These include components such as video or sound cards. However, all assets that store data should be tracked regardless of cost. Examples include:

1. Hard Drives
2. Temporary storage drives
3. Tapes - including system backup data.
4. Although not specifically tracked, other storage devices such as CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes (see Section 3.3 below).

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

Trustees of the devices must sign for receipt of the 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 the following guidelines:

1. Never place sensitive data on a device or media without authorization. Once permission has been obtained, the data-bearing item must be kept in a secure area.
2. Never use these devices to download executable programs from outside the network without prior authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any software brought into the network should be on the IT department's approved list.

The Memory Device Trustee Agreement requires employees to sign for receipt of these devices and agree to handle these assets in accordance with the terms of this policy. This form must be executed by all employees that will work with any organizational data on the first day of employment. The form should also be updated whenever and employee receives one or more memory sticks, temporary storage drives, or data backup drives.

4.0 Asset Tracking Requirements

1. All assets must be assigned 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 in order 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 number will be assigned to the asset and the relevant information shall be entered in the asset tracking database.

5.0 Transfer Procedure:

1. Asset Transfer Checklist – When an asset listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Checklist must be completed by the trustee of the item and approved by an authorized representative of the organization. The trustee is the person in whose care the item resides. 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. The following information must be included:

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

   Once the trustee fills out and signs the Asset Transfer Checklist form, it must be signed by an authorized representative.

2. Data entry - After the Asset Transfer Checklist has been completed, it will be submitted to the asset tracking database manager. The asset tracking database manager will ensure that the information on the form is entered into the asset tracking database within one week.

3. Checking the database - Managers who oversee projects that result in a change to equipment location should check periodically to see if the assets that were moved have been updated in the asset tracking database. The database should include a recent move list that can be easily checked.

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 resigns or is terminated
4. Asset disposal, including:
    - Asset returned to manufacturer or reseller due to warranty return
    - Leased asset returned to Lessor

In all cases the asset transfer checklist must be completed.

7.0 Media Sanitization

When transferring assets to another trustee, any confidential information on the device must be protected and/or destroyed. The method of data destruction is dependent upon the sensitivity of the data on the device and the next user of the device (i.e. within the organization and its control or outside the organization).

Please refer to NIST Special Publication 800-88 Revision 1 "Guidelines for Media Sanitization" in order to select which methods are appropriate to your organization's level of risk tolerance.

8.0 Asset Disposal

Asset disposal is a special case since all sensitive data must be removed during or prior to disposal. The manager of the user of the asset should determine the level of sensitivity of the data stored on the device. The data erasure requirements for the device are based upon the sensitivity of the data as determined during the data assessment process:

1. **None** (Unclassified) - No requirement to erase data. However, in the interest of prudence normally erase the data using any available means such as software-based sanitization, physical destruction, or degaussing.

2. **Low** (Sensitive) - Erase the data using any available means such as sanitization, physical destruction, or degaussing.

3. **Medium** (Confidential) - The data must be erased using an approved technology in order to ensure that data is not recoverable using advanced forensic techniques.

4. **High** (Secret) - The data must be erased using an approved technology to ensure that the data is not recoverable using advanced forensic. Approved technologies are to be specified in a Media Data Removal Procedure document. Asset types include:

    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.

9.0 Media Use

This policy defines the types of data that may be stored on removable media, whether that media may be removed from a physically-secure facility, and under what conditions such removal would be permitted.

Removable media includes the following:

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

Removable media should be handled according to the sensitivity of data stored on the device as determined by the data assessment process:

1. **Unclassified** - Data may be removed with approval by the first level manager and the permission is perpetual for the employee throughout the 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. Approvals are effective on a one-time bases only.

3. **Confidential** - The data may only be removed from secure areas with the permission of a Vice President or higher level of management. Procedures for maintain data security while in transit and at the new destination of the media must be documented.

4. **Secret** - The data may only be removed from secure areas with the permission of the President or higher level of management. Procedures for maintain data security while in transit and at the new destination of the media must be documented

5. **Top Secret** - The data may never be removed from secure areas.

10.0 Enforcement

Because data security and resource protection are critical to the organization, employees that do not adhere to the foregoing policy may be subject to disciplinary action - up to and including termination of employment. Any employee who becomes aware of any violation of this policy is required to report such violation to their supervisor or other another authorized representative of the organization.

11.0 Employee Training and Acknowledgment of Policy

Each employee in the organization is expected to be aware of current policies and procedures related to IT Security and shall be trained on these policies and procedures on at least an annual basis. Employees are required to sign an acknowledgment that they are aware of the policy and will fully comply with its requirements.