Asset Management Policy

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC004	Approved By:	IT&S Steering Committee 3/24/2021 IT Board 4/8/2021
Owner:	IT&S	Effective Date:	4/8/2021

Revision History

Date	Version	Created by	Description of change

Table of Contents

1. Purpose and Scope

The purpose of this document is to provide guidelines for the management and accountability of information and technology assets. The purpose of this policy is to establish the proper criteria and procedures surrounding the acquisition, inventory, and maintenance of organizational assets, thus ensuring their secure and adequate management. City of Helena/Lewis and Clark County IT&S (IT&S) is committed to maintaining a detailed inventory of all IT assets, such as servers, computers, networking equipment, and storage devices.

2. Roles and Responsibilities

Roles and Responsibilities	
IT Director	• Overseeing the management of IT Assets. • Serving as a resource for information Owners and Users on the use of technical controls for the proper handling and protection of data. • Approving IT purchases. • Approving the IT asset disposal list created and maintained by the Helpdesk. • Ensuring compliance with the requirements of this policy to support the security of IT&S assets. • Other responsibilities that relate to asset management.

IT&S Department	• Supporting the management of all components of the IT asset lifecycle, including but not limited to:
	• Overseeing, or delegating, the management of all components of the IT asset lifecycle, including but not limited to:
	  ○ Implementation
	  ○ Installation
	  ○ Asset Maintenance
	  ○ Asset Accountability
	  ○ Asset Disposal
	• Ensuring the inventory of IT assets is up to date and complete.
	• Implementing technical controls to support secure handling and protection of data.
	• Notifying personnel such as the IT Director, or the legal owner, of discrepancies, disposals, or damages involving organizational IT assets.

Asset & Information Owners	• Reporting any loss, theft, or damage of IT&S IT assets to IT&S. • Classifying information and IT assets in accordance with the requirements of this policy • Initial classification and review of classification to ensure accuracy • Following the handling, labeling, and controls identified in this policy
Employee/Users	• Using information assets solely as required for business activities and in accordance with the rules and guidelines of IT&S policies • Following the labeling and secure handling requirements as defined in this policy • Reporting any loss, theft, or damage of IT&S IT assets to IT&S.

2.1 Ownership of Assets

The term "owner" refers to the individual(s) or business unit(s) who have the authority and responsibility for properly classifying and managing IT and information assets.
These individuals or business units are responsible for ensuring:

- That IT assets are inventoried in accordance with the requirements discussed in this policy;
- That assets are appropriately classified, handled and protected in accordance with this policy and other policies, including but not limited to:
    - Access Control and Authorization Policy
    - Data Integrity and Encryption Policy
    - Acceptable Use Policy

3. Data Classification

All IT&S information assets require an assigned classification level. The classification level must consider the impact of disclosure, the degree of sensitivity, and any legal or contractual obligations relevant to the information asset. Information assets should be analyzed to determine their level of sensitivity and criticality in accordance with the classification model outlined below. All information assets must be clearly and appropriately labeled with the assigned classification level.

Data Classification Model		
Classification Level	**Definition**	**Examples**
Confidential	Any information that is extremely sensitive in nature, including but not limited to regulated data, sensitive client information, financial information, or proprietary data. Unauthorized internal or external access to this data could have a major impact on the company. Strict rules should be adhered to in the usage of this data, including any specific rules imposed by the applicable laws, regulations, and/or contracts.	• PII data • ePHI • Credit card information • Financial information, such as billing info. • Payroll data • Social Security Numbers • Administrative passwords or administrative access information • Source code • Customer data • Penetration test or vulnerability assessment results • Any other regulated data • Network maps
Restricted	Any information that is not considered confidential but should be restricted to specific personnel or groups should be considered restricted. This will include but is not limited to network architecture, general security concerns, company pricing information, client lists, or any other relevant information that is not available to the public.	• User ID's and passwords • Client lists • Pricing schemes • Personnel records software and hardware information • File Access Rights
Internal	Any information relating to internal company operations, which is not available to the public. External access to this information is to be prevented, but if it became public, the consequences are not critical and would have limited impact.	• Company general emails • Company calendar • IT&S policies and procedures • Intranet site • Insert additional internal data as relevant

Public	Information available to the public without restriction. Such information will not have adverse effects on the organization if exposed to the public	• Public Facing Web Content • IT&S contact information • Marketing Material

3.1 Initial Asset Classification and Review

IT&S employees are responsible for recognizing the classification level of information assets and taking appropriate actions in accordance with this policy. As applicable, employees will receive orientation from IT&S staff to review IT&S Policies, including the information classification and handling requirements of this policy. The IT&S Policies Acknowledgement form agreeing to adhere to the City/County policies must be signed. All employees will be trained on the classification, labeling, and handling requirements of this policy as part of initial and recurring training.

Additionally, the classification levels of IT&S information assets must be reviewed periodically to ensure classifications are still accurate and identify any needed changes. The information owner is responsible for such review.

4. Labeling of Information Assets

All information assets must be clearly and appropriately labeled with the assigned classification level.

- **Public information** – no labeling requirements. However, adding the label "Public" (or "Unrestricted") is advisable if possible – to avoid confusion.
- **Internal, Restricted, and Confidential information** – should be labeled with the appropriate classification name. If a document contains data in different classification levels, the highest level of classification will determine the classification of the document and the appropriate label.
- Classification labels in electronic documents should appear on every page when the document is viewed or printed. This can be achieved by adding a header and/or footer to the document indicating the classification level.
- Classification labels on removable/portable media should be clearly visible.

5. Handling of Information Assets

The following table provides the requirements for handling assets and data based on the classification level. If an asset contains data in different classification levels, the highest level of classification will determine the classification of the asset and the appropriate handling requirements.

Activity	SECURITY CONTROLS BY CLASSIFICATION LEVEL		
	Confidential	Restricted / Internal	Public
Electronic Document Storage	Information must be stored on company-owned devices. Data must be encrypted using approved encryption methods in accordance with the Data Integrity and Encryption Policy. Media must be secured in a locked storage area when not in use.	Information must be stored on company-owned devices. Devices must be secured from unauthorized access.	No requirements. The data can be shared.
Hard Copy (printed material)	Must not be left unattended in areas with public access. Must be stored in a locked container or cabinet, or in an office area with restricted access. Must be destroyed using a shredder or placed in central shredding bins that are shredded routinely.	Must not be left unattended in areas with public access. The document must be stored in a locked cabinet	No requirements. The document can be shared.

Activity	SECURITY CONTROLS BY CLASSIFICATION LEVEL		
	Confidential	Restricted / Internal	Public
Electronic Transfer (i.e. Email, SFTP)	Transfer to internal or external parties must be done based on a need-to-know. Transfer to external parties requires an NDA and approval from the data owner. Minimum 128-bit encryption (e.g. SSL/TLS) is required for all communications outside of an IT&S network. Encryption (e.g. SSL/TLS) is required for all communications outside of an IT&S network and must meet the requirements of the Data Integrity and Encryption Policy.	Must be transferred internally to only authorized personnel. When files are transmitted, they must be securely protected Transfer to external parties requires an NDA. Minimum 128-bit encryption (e.g. SSL/TLS) is required for all communications outside of an IT&S network.	No requirements
Information Systems	Only authorized persons may have access. Access must be restricted based on the principal of least privilege and in accordance with the Access Control and Authorization Policy. Access to the information system must be protected by a strong password. The system should be configured to automatically lock or terminate inactive session after 15 minutes of inactivity.	The information system must be protected from external access and password protected. Users must use care to prevent shoulder-surfing or other viewing by unauthorized users and must lock device screens when unattended.	No Requirements
Disposal of Information (electronic)	In addition to removing the file, the space used by the file must be overwritten or formatted using approved means. (permanent destruction) Data must only be deleted after the information's retention period.	Files/data must be removed via the system's "delete" or "remove" function.	No Requirements

Activity	SECURITY CONTROLS BY CLASSIFICATION LEVEL		
	Confidential	Restricted / Internal	Public
Disposal of Physical Medium (e.g., paper/magnetic media)	ALL media must be disposed of securely using approved methods (e.g. shredding, overwriting of magnetic media) and based on retention strategies. A record of media disposals must be maintained by IT&S.	Media must be disposed of securely using approved methods (e.g. shredding, overwriting of magnetic media) and based on retention strategies.	No Requirements

6. Systems Classification

In conjunction with risk analysis activities, a criticality analysis will be performed to determine the criticality of IT&S systems to business operations.

IT&S will inventory all information systems, as well as identify and document dependencies between systems. Using this information, the IT Director (and Security Officer) will classify each system by criticality, with input from relevant departments, subject matter experts, and management as needed. The following table outlines the varying impact of system unavailability, or how critical the system is.

Criticality Level	Description	Time in which incident must be addressed
High	Loss of system availability could result in a severe business impact.	Incident must be addressed immediately
Medium	System unavailability could result in significant loss of operations.	Incident must be addressed within 2 hours
Low	System unavailability could result in a limited impact to individual users or department.	Incident must be addressed within 24 hours
Minimal	System unavailability results in virtually no impact to operations, users, or departments.	Incident may be addressed when convenient

The Security Officer will coordinate the documentation of the results of the system criticality analysis in a list of critical systems, which will be used to support contingency planning and the prioritization of recovery activities. This document will contain:

- The criticality level of each system
- The corresponding system owner
- Business function
- System dependencies
- Information asset(s) stored, processed, transmitted, or created on the system

7. Device and Media Controls

This section outlines the implementation, destruction and re-use of IT&S's media devices. These devices include but are not limited to:

- Servers
- Terminals
- Workstations/laptops
- Mobile phones/tablets
- Portable storage media (i.e. USB drives, SD cards)
- External hard drives
- Networking equipment
- Software and licenses
- Databases
- Output devices (i.e. scanners, photocopiers, printers, fax machines)

7.1 Acquisition

The IT Director or designated IT staff must approve all equipment purchases. Requests for the purchase of new equipment must be sent to the IT Director or designated IT staff as a Hardware Request Form. All monies for spending must be pre-approved via purchase order by The IT

Director or designated IT staff. The IT Director or designated IT staff must also approve the purchase order.

- Type of Asset requested
- Business justification
- Cost or estimated cost
- Urgency

After the Hardware Request has been approved, the IT Director or designated IT staff will make the purchase or delegate the purchase to another employee.

7.2 Inventory & Accountability

IT&S will maintain a current and accurate inventory if its IT assets to support access to asset information needed for patch and vulnerability management, incident response, and business continuity.

Each asset must be assigned a unique ID. IT&S will keep a record of company information systems (KACE). The IT Director or designated IT staff is responsible for maintaining the inventory, which includes tracking ownership and maintenance of the systems.

Each entry should include the following, if applicable (KACE or CPU Label):

- Asset ID
- Asset classification
- Serial number, manufacturer, model
- Asset owner (indicate the Department to whom the asset has been assigned to)
- Date of purchase
- Description of business function
- Location
- IP Address
- Software and licensing information
- Value of purchase
- Purchase order reference number
- Vendor contact
- Licensing information
- Version and update information.
- System backup and maintenance status
- Service contract or maintenance contract details, if applicable
- Disposal and destruction status, and method of destruction

If information contained within the asset inventory becomes outdated, the IT Director or designated IT staff must make the necessary changes in a timely manner. This will ensure that IT&S has complete knowledge of the current information systems and related activities. The IT Director must coordinate the review of the asset inventory at least annually, to confirm the accuracy of the document.

7.3 Software Application

IT&S will maintain an inventory of its software applications. These software applications include, but are not necessarily limited to, the following:

- Application Software (Licensed)

- Freeware/Shareware
- System Software
- Various Tools
- Databases

This inventory of software applications will adhere to the requirements mentioned above in Inventory and Accountability. Additionally, this inventory will include the following information:

- Pertinent location information of the software;
- Licensing information, including any specific license keys
- Pertinent information relating to its functionality or security (e.g., baseline software configurations, approved deviations, etc.)
- Information needed to support technical vulnerability management

7.4 Management of Removable Media

Use and management of removable media is subject to the following requirements:

- Use of removable media in workstations should be monitored and restricted. Users are only permitted to use removable media if a legitimate business need exists~~.~~ Request and approval of removable media must adhere to the requirements outlined in the Access Control and Authorization Policy and Acceptable Use Policy.
- Only approved removable media devices may be used. Removable media (i.e. USB Drives) may be issued to users by the IT Department and will be tracked to ensure such media is returned for proper disposal and/or removal of data.
- Removable media must not be used in servers unless required for performing specific tasks and removed immediately once completed. Physical access to servers and ports used for removable media must be restricted to authorized personnel only.

7.5 Maintenance and Patch Management

It is essential to the security of IT&S systems and information that all technology assets have the most recent operating system and application updates (aka “patches”) installed.

The Network Manager and Network Staff are responsible for overseeing patch management implementation, procedures, and timing/scheduling of patches. The Network Staff and Network Staff will be responsible for carrying out patch management procedures such as patching servers, workstations, and infrastructure components (switches, routers, etc.). When possible, systems will be configured to accept automatic updates. The Network Manager and Network Staff are responsible for establishing a patch schedule for systems that do not automatically update.

The Network Manager and Network Staff will also consult various resources to stay informed about current security threats and available patches.

The IT Director must approve any off-site maintenance of equipment containing information classified as Internal or Confidential. The data on the device must be backed up and completely wiped from the device prior to taking the device off-site for maintenance.

7.6 Destruction and Disposal

As organizational assets lose functionality or are no longer needed, disposal may be necessary. IT&S will ensure that all information assets are properly destroyed and/or erased when no longer

needed. Disposal of IT&S IT assets must be formally approved by the IT Director. Upon approval, the IT Director or designated IT staff is responsible for the destruction and disposal of media and devices, as well as their removal from the inventory of assets.

Prior to redistribution, salvage, or disposal, all sensitive information must be erased from the specific IT assets. All electronic information must be overwritten bit by bit. IT Staff will confirm through technical testing that removal procedures are successful and complete. Hardware assets to be destroyed may also be disposed through an authorized disposal company. Certificates of destruction must be obtained. Any hardware awaiting destruction or disposal must be stored in a secure area.

7.7 Media Re-use

Some devices, such as hard drives and computers, may be reused after properly removing all sensitive information. IT Staff will ensure that the requirements for removal outlined in the section above, *5.4 Destruction and Disposal,* are applied to all devices before they are made available for reuse.

The Board of County Commission (BOCC) is also responsible for transferring ownership of a reused device in the asset inventory. If media is not intended for recycle or reuse, the best control may be destruction.

7.8 Return of Assets

IT&S employees and certain external party users sometimes have IT assets in their personal possession. For example, IT&S issues laptop computers to certain employees. Upon termination of these individuals' relationships with IT&S these IT assets must be returned.

IT&S must see to it that these IT assets are returned as soon as possible and that IT&S follows any other information security policies relevant to the IT asset's return or the termination of the relationship with the individual.

In the event the individual refuses or is unable to return the IT asset, IT&S is required to abide by its information security policies that apply to such a scenario.

8. Policy Maintenance and Management

The Owner of this document must evaluate and perform any necessary updates to this document at least once per year. The owner may delegate tasks related to this policy.

- The IT Director will adhere to the continual validation, review, and updating of this policy.
- When evaluating this policy, the number of discrepancies within the Inventory of Assets as well as any incidents of unauthorized access, transfer, or disposals must be considered.

9. References

NIST Cybersecurity Framework References

- ID.AM – Asset Management
- PR.IP – Information Protection Processes and Procedures
- PR.DS – Data Security
- PR. MA – Maintenance
- PR.PT – Protective Technology

Policy References

- Access Control and Authorization Policy
- Acceptable Use Policy
- Data Integrity and Encryption Policy