Policy Title Technology Asset Management Policy
Department Information Services
Chapter 5
Section 8
Policy 10
Effective Date Tuesday, June 21, 2022

POLICY STATEMENT

Technology Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critical to maintain updated inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities. In support of these objectives, this policy governs the oversight of tangible information technology equipment.

APPLICABILITY

This policy applies to information technology assets (desktops, laptops, tablets, mobile phones, printers, servers, networking, etc.) and to county-owned storage devices (storage arrays, hard drives, optical media, etc.). This policy addresses requirements in the Health Insurance Portability and Accountability Act (HIPAA), section 164.310(d)(2) and Criminal Justice Information Standard (CJIS) 5.8.4 (Media Protection).

GENERAL INFORMATION

Asset Allocation (desktops and laptops)

Unless HR provides an exception under the American Disabilities Act, Ramsey County will supply each employee one (1) primary computing device. Information Services (IS) standards will determine the type of device, based on business need and operational efficiency.

Asset Tracking Requirements

Asset categories as determined by Finance and IS Finance will be tracked by serial number using a mechanism that allows for easy reference to identifying information, including:

- Date of purchase
- Make, model, and descriptor
- Type of asset (server, storage, etc.)
- Owner
- Department
- Purchase order number
- Disposition (i.e., active, decommissioned, etc.)

Prior to deploying an asset, Information Services shall assign an ID to the asset and enter its information in the asset tracking database. The asset inventory is subject to audits as determined by Finance and IS Finance.

Asset Disposal and Repurposing

Whether internally or via its authorized agent, Ramsey County Information Services will sanitize or destroy media containing sensitive information during the disposal process or before transfer to another department. Ramsey County Information Services or its authorized agent shall comply with **NIST 800-88** or **NAID-AAA** to determine what type of data destruction protocol may be used for erasure or destruction. Acceptable methods are:

Non-CJIS Data:

- physical destruction
- 1-pass data overwrite or degaussing for magnetic media
- ATA SecureErase or ATA SanitizeDisk command for solid state media.

CJIS Data:

- physical destruction
- 3-pass data overwrite or degaussing for magnetic media.
- 3-pass data overwrite for solid state media. Note: CJIS does not adequately address overwriting SSDs. The SSD storage areas may not be accessible via typical three pass overwrite patterns, so an ATASecureErase or ATA SanitizeDisk command should be issued three times. Although NIST 800-88 specifies that a single pass is sufficient to erase solid state memory, three passes should be executed to satisfy the CJIS standard.

If the data classification is unknown and could possibly be CJI, then the media must use the CJIS protocol.

Inoperable digital media that cannot be overwritten, degaussed, or cryptographically erased must be physically destroyed. Media destruction must be witnessed or executed only by authorized personnel on behalf of Ramsey County. A certificate of data/media destruction must be created and filed for any such media.

For data hosted externally, service agreements must stipulate sufficient measures to ensure data sanitization is performed appropriately throughout the system lifecycle.

AUTHORITY

This policy and related standards and procedures were prepared under the authority of the County Manager, as delegated to the Ramsey County Chief Information Officer. Failure to adhere to these policies may result in loss of access privileges and disciplinary action, up to and including termination of employment.

DEFINITIONS

Technology Asset: For the purposes of this policy, an asset is defined as a tangible information technology device, such as a server, a laptop, or a hard drive.

3-pass data overwrite: Department of Defense 5220.22-M data sanitization method defines a 3-pass overwrite as:

- Pass 1: Overwrite all addressable locations with binary zeroes.
- Pass 2: Overwrite all addressable locations with binary ones.
- Pass 3: Overwrite all addressable locations with a random bit pattern.

Degaussing: The destruction of the data on a data storage device by removing its magnetism.

Physical destruction: A method of permanently destroying physical media through incineration or pulverization to render data recovery impossible.

Cryptographic Erasure: A method of sanitization in which the media encryption key for the encrypted target data is sanitized, making recovery of the decrypted target data infeasible.

Primary Computing Device: A Ramsey County issued desktop or laptop with which an employee is expected to perform at least 80% of their work. Mobile devices such as tablets and phones are not considered primary computing devices.

RESPONSIBILITIES

Ramsey County

1. Ensure the physical security of its information system assets.
2. Investigate violations as needed or directed to protect its data and resources or to provide information relevant to an investigation.

Information Services

1. Identify and maintain acceptable data destruction techniques in accordance with regulations that govern that data.
2. Enforce identified data destruction and asset disposal practices.

Finance and IS Finance

1. Identify and maintain the fields in the asset inventory.
2. Oversee audits to confirm the accuracy of the asset inventory.

Designated support teams (Information Services and business)

Ramsey County has a tightly federated technology support model. The following groups are responsible for managing assets in their areas of responsibility. Each of these groups is responsible for managing their assets and data in compliance with this policy.

1. IS infrastructure system administrator manages most of the Microsoft Windows Server, MS database, and MS backup office technologies.
2. IS infrastructure network administrator manages most of the Cisco network solutions.
3. IS desktop support manages most of the desktop and peripheral devices.
4. Sheriff's Office, Office of Information & Technology, manages a variety of technologies server, desktop, peripherals, and networks.
5. Library Services, Office of Information & Technology, manages a variety of technologies, including servers, desktops, peripherals, and networks.
6. Application support and capability teams maintain a subset of applications and business services.
7. Vendors manage a variety of 3rd party-supported technologies, including servers, desktops, peripherals, and networks.

Users

1. When no longer required, return technology assets to Information Services or an authorized contact.

LINKS AND RESOURCES

› **IT Hardware-Software Standard**

› **Acceptable Use of Information Technology Resources Policy**

› **IT Hardware-Software Replacement Program Overview**

› **CJIS Security Policy**

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
June 21, 2022	Initial version

APPROVAL

Chetan Ganatra, Ramsey County Chief Information Officer

June 21, 2022

Revision History Date Thursday, June 30, 2022

‹ Encryption at Rest Back Section 9 - Incident Management ›