Policy Title Cloud and Removable Media Policy
Department Information Services
Chapter 5
Section 4
Policy 2
Effective Date Monday, February 1, 2021

POLICY STATEMENT

Ramsey County is accountable for securing private, sensitive, and confidential information that if lost or improperly disseminated could violate the law. County employees are responsible for preventing the loss or unauthorized disclosure of this information. Consequently, Ramsey County data may not be stored on removable media or in the cloud except as allowed below, regardless of data classification level.

APPLICABILITY

This policy applies to all Ramsey County employees, which for the purposes of this policy includes interns, consultants, contractors, and elected and appointed officials with access to Ramsey County information technology resources. This policy addresses chain of custody and data security controls as referenced in HIPAA §164.310(d)(1).

GENERAL INFORMATION

Removable Media: Except as noted below, Ramsey County prohibits data storage on removable media such as compact discs, DVDs, external hard drives, and USB drives. Exceptions include instances where a department has identified a standard solution and has implemented adequate security controls to protect the data on those external devices. In all instances where data is kept on removable devices, access and chain of custody must be closely controlled.

Even where removable media is permitted, employees are not permitted to copy County data to external storage outside of any of the approved processes. Examples of prohibited functions include keeping a privately-owned USB drive attached to a laptop as a document repository for County data or making an image of the laptop on a DVD that's kept at home. In these instances, Ramsey County does not own the devices and cannot guarantee the security of the data.

Aside from data loss and chain of custody concerns, USB thumb drives can transmit malware, infecting anything they're plugged into and potentially spreading through the Ramsey County network. For this reason, only Ramsey County approved thumb drives may be used for desktops and laptops and must be encrypted to prevent unauthorized access.

General Cloud Storage: Ramsey County data may not be kept on general-purpose cloud storage platforms (i.e.Dropbox, Box, Apple iCloud, Google Cloud, Microsoft OneDrive) unless these platforms are approved by Information Services. Microsoft OneDrive associated with Ramsey County usernames are approved. Personal instances of Microsoft OneDrive as well as the other solutions listed above are not approved.

Private devices such as laptops and desktops are permitted to access Ramsey County cloud storage only when following the standards and procedures developed by Information Services.

Cloud Applications: Approved software-as-a-service applications that run in the cloud usually include their own storage capabilities, and insofar as these applications are approved by Ramsey County Information Services, these storage locations are permitted for the purposes intended. An example is the NextGen healthcare platform.

AUTHORITY

This policy was prepared under the authority of the County Manager, as delegated to the Ramsey County Chief Information Officer. Failure to comply with this policy may result in the suspension of use and connectivity privileges. It may also result in disciplinary action, up to and including termination of employment.

RESPONSIBILITIES

Ramsey County

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

Departments

1. Ensure covered individuals have read and understand this policy and related standards.
2. Refer expected violations of County information technology policies and any vulnerabilities in County information systems to Information Security at **ISSecurity-DL@co.ramsey.mn.us**.

Designated support teams (Information Services and business)

Ramsey County has a distributed technology infrastructure support model. The following groups are responsible for enforcing this policy within their domain of responsibility.

1. IS Infrastructure system administrators manage most of the servers and backups.

2. IS desktop support manages most of the desktop and peripheral devices.
3. Sheriff's Office, Office of Information & Technology, manages a variety of technologies server, desktop, peripherals, and networks.
4. Library Services, Office of Information & Technology, manages a variety of technologies, including servers, desktops, peripherals, and networks.

Each of the above-referenced support teams will:

- Review exception requests to this policy.
- Not attach any storage device to a Ramsey County asset that isn't approved by Information Services.
- Investigate violations, either through routine system administration or from complaints, and take necessary actions to protect county resources or to provide information relevant to an investigation.

Users

1. Understand and comply with this policy and all related policies and standards. Use only authorized storage devices for Ramsey County data.
2. Do not attach any device to a Ramsey County asset that isn't approved by Information Services.
3. Acquire technology solutions via the Procurement and Information Services department defined processes.
4. Cooperate with investigations of potential unauthorized or illegal use of Ramsey County IT resources.

LINKS AND RESOURCES

- Remote Working & Mobile Device Policy

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
Feb 1, 2021	Initial version

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, February 1, 2021
Revision History Date Monday, February 8, 2021