Policy Title Sensitive Electronic Data Protection Policy
Department Information Services
Chapter 5
Section 7
Policy 3
Effective Date Wednesday, February 3, 2021

Ramsey County maintains private and sensitive information pertaining to healthcare, criminal justice, payment cards, and other local, state, and federal programs. To minimize risk to the county and its residents, sensitive information must be protected from accidental and malicious disclosure or destruction. This policy identifies the high-level security controls required to protect this sensitive data.

APPLICABILITY

This policy applies to all electronic information classified as sensitive, confidential, or private. Users and administrators of this data are bound to the requirements specified within this policy. All systems that host or access this information, whether local or remote, must be configured in accordance with this policy.

This policy applies to the HIPAA Security Rule, the HIPAA Privacy Rule, Payment Card Industry Data Security Standard (PCI-DSS), Criminal Justice Information Services guidelines (CJIS), personally identifiable information (PII), and potentially other regulations and guidelines that address the security of sensitive, confidential, and private data.

GENERAL INFORMATION

Administrative Controls

Ramsey County data owners, data stewards, and compliance officers shall ensure policies and procedures govern the collection, use, processing, storing, transmitting, and disclosing of sensitive information. Specifically:

- All devices that access sensitive information shall have professional technical support sufficient to maintain information security.
- Electronic records containing sensitive information should exist only in areas where there is a legitimate and justifiable business need.
- Policies and procedures will be clear, reasonable, and protect the county and individuals.
- Controls will be adequate, relevant, and not excessive.
- Appropriate consent shall be obtained before collecting, using, and disclosing sensitive information.
- Sensitive information will be processed in accordance with federal and state regulations, statutes, and laws.
- Assets and information will be transferred only to areas with adequate protection as summarized below.

Technical Controls

The designated support teams as listed in Responsibilities will ensure that sensitive electronic data is protected as outlined in the policies below and with any standards associated with these policies.

Employee Screening Policy (4.1.1)

- Employees with access to sensitive data must complete a background check before they are granted access to that data.

Security Training & Awareness Policy (5.1.2)

- Employees with access to sensitive information will complete information security training relevant to their access.

Access Control Policy (5.2.1)

- Access to sensitive data will be limited to those who need to know.
- Access to sensitive data shall be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user.
- Host security log files must be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event.
- System and application owners shall conduct periodic reviews of information systems in their control that contain sensitive information and adjust controls and procedures as appropriate.

Privileged Access Control Policy (5.2.2)

- Administrative passwords should be exceptionally strong. User accounts with fewer privileges should be used instead of administrative accounts whenever possible. Periodic review of access privileges and account scavenging is required.

Physical Security Policy & Remote Working Policy (5.4.1)

- Physical access to computers and related infrastructure shall be restricted to the degree possible.

Removable & Cloud Media Policy (5.4.2)

- Use of portable flash media is forbidden without prior approval from the Chief Information Officer.

Asset Management Policy (5.6.1)

- A secure deletion mechanism shall be used to erase unencrypted data from media prior to transfer, surplus, or disposal of hardware. Unencrypted, non-erasable media must be destroyed.

Data Classification Policy (5.7.2)

- Sensitive data must be classified as such so that the appropriate controls can be enforced.

Patch Management Policy (5.8.1)

- Systems and software will be scanned for vulnerabilities and patched regularly to protect data.

Backup & Restore Policy (5.8.3)

- Periodic backup copies of software and data must be made, tested, and stored securely.

Disaster Recovery and Business Continuity Policy (5.8.4)

- To ensure high availability of ePHI, systems and applications should be tolerant to component failure and broader outages.

Incident Management Policy (5.8.5)

- A procedure must exist for responding to security incidents involving sensitive data.

Configuration Management Policy (5.8.6)

- Hosting devices will adhere to information security standards.
- Data must be stored on hardened file servers and databases.
- Desktop/laptop/server screens will lock after a period of inactivity, requiring reauthentication to gain access.

Secure Data Transmission Policy (5.8.7)

- All external transmission across open networks shall require both the authentication data (e.g. user ID and password) and the data itself to be encrypted with strong encryption.

AV/Malicious Code Policy (5.8.8)

- Systems that store or process sensitive information will be protected from malicious software.

Network Security Policy (5.8.9)

- Networks will be secured from unauthorized access and segmented from insecure and public-facing networks.

Encryption at Rest Policy (5.8.13)

- Sensitive data will be encrypted at rest.

Physical Security Policy (7.1.3)

- Systems hosting or transmitting sensitive data must be physically secured from unauthorized access and must be reasonably secured from natural and environmental hazards.

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 disciplinary action, up to and including termination of employment.

DEFINITIONS

The following definitions are in the **Information Services Data Dictionary**:

Sensitive Data: Electronic information with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security-related data. It also includes data that is not open to public examination because it contains information which, if disclosed, could cause severe reputation, monetary or legal damage to individuals or the county or compromise public activities. Examples include: passwords, intellectual property, ongoing legal investigations, medical information, social security numbers, birth dates, bank or credit card account numbers, income and credit history.

RESPONSIBILITIES

Ramsey County

1. Ensure the confidentiality, integrity, and availability of its systems and data.

Departments

1. Understand and comply with county policies, standards, guidelines and procedures governing the security of sensitive data within their department.
2. Identify a Department Privacy Contact who will assemble any data as part of a formal data request and ensure any released data is released appropriately.

Information Services

1. Develop, implement, and enforce technical controls for sensitive data and document these controls in policies and standards.

Designated Support Teams (Information Services and Business)

Ramsey County has a distributed technology infrastructure support model. The following groups are responsible for managing systems in their designated domain of responsibility.

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, including 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 Ramsey County applications and services.
7. Vendors manage a variety of 3rd party-supported technologies, including servers, desktops, peripherals, and networks.

Each of the above-referenced support teams will:

1. Ensure that all department-maintained hardware and software comply with policies and standards that govern sensitive data.
2. Report systems and applications that are not compliant to the Ramsey County Data Compliance Officer.

LINKS AND RESOURCES

- **Employee Screening Policy (4.1.1)**
- **Security Training & Awareness Policy (5.1.2)**
- **Access Control Policy (5.2.1)**
- **Privileged Access Control Policy (5.2.2)**
- **Remote Working Policy (5.4.1)**
- Removable & Cloud Media Policy (5.4.2)
- Asset Management Policy (5.6.1)
- Data Classification Policy (5.7.2)
- **Patch Management Policy (5.8.1)**
- Backup & Restore Policy (5.8.3)
- Disaster Recovery and Business Continuity Policy (5.8.4)
- Incident Management Policy (5.8.5)
- **Configuration Management Policy (5.8.6)**
- **Secure Data Transmission Policy (5.8.7)**
- AV/Malicious Code Policy (5.8.8)
- Network Security Policy (5.8.9)
- Encryption at Rest Policy (5.8.13)
- Physical Security Policy (7.1.3)

CONTACTS / SUBJECT MATTER EXPERTS

- Ramsey County Chief Information Security Officer
- Ramsey County Chief Compliance and Ethics Officer

REVISION HISTORY

Date	Brief description of change
Feb. 3, 2021	Initial version

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, Feb 3, 2021

Deanna Pesik, Chief Compliance and Ethics Officer, Feb 3, 2021
Revision History Date Tuesday, February 9, 2021