Policy Title Encryption at Rest
Department Information Services
Chapter 5
Section 8
Policy 13
Effective Date Wednesday, July 28, 2021

POLICY STATEMENT

When sensitive data is at rest (i.e., stored digitally) outside the boundary of the physically secure location (i.e., Ramsey County offices), the data shall be protected via encryption. The encryption and decryption mechanisms must be documented and secured from unauthorized access.

APPLICABILITY

The policy applies to the following regulated data:

- Electronic Health Care Information (ePHI) as governed by the Healthcare Information Portability and Accountability Act (HIPAA) and the Minnesota Government Data Practices Act. The specific HIPAA sections are § 45 CFR 164.312(a)(2)(iv) and § 45 CFR 164.312(e)(2)(ii).
- Payment Card Industry (PCI), which pertains to credit cards, bank cards, and related instruments. This is governed by the Minnesota Government Data Practices Act.
- Criminal Justice Information (CJI) as governed by the Criminal Justice Information Standard (CJIS) and the Minnesota Government Data Practices Act. The specific CJIS section is 5.10.1.2.2 (Encryption for CJI at rest).
- Personally Identifiable Information (PII), which pertains to birthdates, social security numbers, addresses, and related data. This is governed by the Minnesota Government Data Practices Act.

GENERAL INFORMATION

When encryption is employed, the cryptographic module used shall be Federal Information Processing Standards (FIPS) 140-2 certified and use a symmetric cipher key strength of at least 128-bit strength or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256-bit strength.

The passphrase used to unlock the cipher shall meet the following requirements:

1. Be at least 10 characters
2. Not be a dictionary word.
3. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
4. Be changed when previously authorized personnel no longer require access.

Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in the Ramsey County **Access Control Policy** shall be applied.

Encryption keys will be stored in one or more key management systems that meet the following security requirements:

1. Information Services shall safeguard the security of encryption keys to ensure that they remain confidential and available.
2. Key management should be fully automated so that systems administrators do not have the opportunity to expose a key or influence the key creation.
3. Keys in storage and transit must be encrypted.
4. Decryption keys shall not be associated with user accounts.
5. Documentation and procedures are required to protect keys.
6. Access to cryptographic keys will be restricted to the fewest number of custodians necessary.
7. Cryptographic keys will be stored in the fewest possible locations.
8. Keys will be retired, replaced, or archived when the integrity of the key has been weakened or keys are suspected of being compromised.
9. Cryptographic key custodians shall formally acknowledge that they understand and accept their key-custodian responsibilities.

The Chief Information Security Officer will be the sole approver for any exceptions to this policy. Exceptions will be recorded as a risk record and will be periodically reviewed for continued necessity.

AUTHORITY

This policy and the procedures herein were prepared under the authority of the county manager, as delegated to the Ramsey County Chief Information Officer.

DEFINITIONS

- Encryption: The conversion of data from a readable format into an encoded format that can be read or processed only after it's been decrypted.
- Passphrase: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

- Electronic Private Healthcare information (ePHI): Protected health information (PHI) that is produced, saved, transferred, or received in an electronic form. In the United States, ePHI management is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.
- Payment Card Industry information (PCI): This is information that includes cardholder data such as the cardholder's name, the primary account number, and the card's expiration date and security code.
- Criminal Justice Information (CJI): Information collected by criminal justice agencies needed for the performance of their legally authorized, required function. Examples include vehicle registration, driver license information, crime and arrest records, wanted persons, and more.
- Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by direct or indirect means.

RESPONSIBILITIES

Ramsey County

Ensure the security of data, systems, and users' accounts within Ramsey County. Investigate violations as needed or directed to protect county data and resources or to provide information relevant to an investigation.

Departments

Investigate alleged violations of Ramsey County information technology policies. Report any known weakness or vulnerability in Ramsey County information system security or compliance as outlined in procedures.

Application and Data Owners

Data Owners are accountable to ensure that the data they own is stored only in authorized containers, such as properly configured databases, file shares, and MS Teams/SharePoint/OneDrive. Local drives (i.e., C drive) and USB drives are not authorized containers and should never contain protected data. Ramsey County Information Services will not encrypt unauthorized containers.

Application and data owners will provide evidence of compliance to Information Services or an authorized auditor when requested.

Designated support teams (Information Services and business)

Ramsey County has a distributed technology infrastructure support model. The following groups are responsible for encrypting data at rest AFTER the data owner has identified and classified the data to be encrypted.

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

Each of the above-referenced support teams will ensure that managed applications and technology infrastructure comply with this policy insofar as they encrypt sensitive data that is stored on devices outside of Ramsey County's physical security controls and that cryptographic key management procedures meet the security requirements outlined above. They will provide evidence of policy compliance to Information Services or an authorized auditor when requested.

LINKS AND RESOURCES

› **Secure Data Transmission Policy**

› **Access Control Policy**

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
July 28. 2021	Intial version, reviewed by Rich Christensen, Eric Brown, Chris Bogut, Marc Dronen, Teal Girgen

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, July 28, 2021
Revision History Date Thursday, July 29, 2021