Policy Title Secure Data Transmission
Department Information Services
Chapter 5
Section 8
Policy 7
Effective Date Friday, December 18, 2020

POLICY STATEMENT

Private, confidential, and sensitive data, including ePHI, PCI, and PII, within control of Ramsey County must incorporate data integrity and authentication controls while in transit. Further, this same data must not leave Ramsey County in an unencrypted state and must be encrypted if it traverses public networks such as the Internet, wireless, Bluetooth, and cellular. The encryption and decryption mechanisms must be documented and secured from unauthorized access.

APPLICABILITY

The policy is applicable to all ePHI, PCI, CJI, and PII data. This policy is applicable to data-in-transit requirements that are mandated by HIPAA, Minnesota Government Data Practices Act, Minnesota health regulations, PCI-DSS, and Department of Homeland Security. The specific HIPAA sections are § 45 CFR 164.312(a)(2)(iv) and § 45 CFR 164.312(e)(2)(ii).

GENERAL INFORMATION

Personal, healthcare, financial, criminal, and other confidential information must be protected from unauthorized access and alteration while it is being transmitted. Ramsey County is committed to protecting the confidentiality and integrity of this information through technical and administrative controls.

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

The following terms are defined in the **Information Services Data Dictionary**:

- Electronic Private Healthcare information (ePHI)
- Payment Card Industry information (PCI)
- Criminal Justice Information (CJI)
- Personally Identifiable Information (PII)

RESPONSIBILITIES

Ramsey County

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

Departments

1. 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 Owners

Application owners will ensure that managed applications comply with this policy insofar as they ensure the integrity of transmitted data and encrypt sensitive data over public networks. 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 managing privileged access control in their designated domain of responsibility.

- IS infrastructure system administrator manages most of the Microsoft Windows Server, MS database, and MS backup office technologies.
- IS infrastructure network administrator manages most of the Cisco network solutions.
- IS desktop support manages 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 applications and business services.
- Vendors manage a variety of 3rd party-supported technologies, including servers, desktops, peripherals, and networks.

1. Each of the above-reference support teams will ensure that managed applications and technology infrastructure comply with this policy insofar as they ensure the integrity of transmitted data and encrypt sensitive data over public networks, specifically:
    a. Require strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, SFTP, etc.) to safeguard confidential information or PII during transmission over open public networks.
    b. Accept only trusted keys and certificates.
    c. Encrypt confidential Information transmitted in e-mail messages.
    d. Encrypt wireless transmissions of confidential information using current, standard protocols.
    e. Encrypt connections from Bluetooth devices.
    f. Use encryption keys that meet Ramsey County and industry standards for length and complexity.
    g. Encrypt all non-console administrative access such as browser/web based management tools for applications and infrastructure.
2. Cryptographic key management procedures must ensure that authorized users can encrypt and decrypt all confidential information using controls that meet operational needs. Key management systems must meet the following security requirements:
    a. Information Services shall safeguard the security of encryption keys to ensure that they remain confidential and available.
    b. Key management should be fully automated so that systems administrators do not have the opportunity to expose a key or influence the key creation.
    c. Keys in storage and transit must be encrypted.
    d. Decryption keys shall not be associated with user accounts.
    e. Documentation and procedures are required to protect keys.
    f. Access to cryptographic keys will be restricted to the fewest number of custodians necessary.
    g. Cryptographic keys will be stored in the fewest possible locations.
    h. Keys will be retired, replaced, or archived when the integrity of the key has been weakened or keys are suspected of being compromised.
    i. Cryptographic key custodians shall formally acknowledge that they understand and accept their key-custodian responsibilities.
3. Provide evidence of policy compliance to Information Services or an authorized auditor when requested.

LINKS AND RESOURCES

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
Dec. 7, 2020	Initial version, reviewed by Rich Christensen, Eric Brown, Chris Bogut and Marc Dronen.

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, Nov. 13, 2020

Revision History Date Friday, December 18, 2020

‹ IT Hardware-Software Standard **Back** **Malware Protection Policy ›**