Policy Title Configuration Management Policy
Department Information Services
Chapter 5
Section 8
Policy 6
Effective Date Friday, November 13, 2020

POLICY STATEMENT

Ramsey County is committed to and responsible for ensuring the confidentiality, integrity and availability of the data and information stored in its systems. System configuration management is a best practice designed to prevent exploitation of IT vulnerabilities that may exist within an organization.

All Ramsey County information technology system components and software must be configured to minimize security vulnerabilities. Only required software and services may run on these systems, and all applications will be configured securely. Further, only IS-approved devices can connect to the Ramsey County production network.

APPLICABILITY

This policy is applicable to all information technology assets connected to the Ramsey County network, or owned, maintained, utilized by or otherwise under the control of Ramsey County, and the administrators of all such systems and networks. This includes third-party externally hosted applications. Roles and responsibilities are determined by application owner and support model.

This policy is relevant to Criminal Justice Information Services (CJIS) section 5.7 (Configuration Management). Configuration management is not specifically mentioned in the Health Insurance & Accountability Act (HIPAA) Security Rule, although the identification of vulnerabilities is covered in the HIPAA administrative safeguards under the security management process standard, in general: 45 C.F.R. § 164.308(a)(1)(i) as well as 45 C.F.R. § 164.308(a)(5)(ii)(B) – protection from malicious software – and 45 C.F.R. § 164.308(a)(8) – the evaluation standard.

GENERAL INFORMATION

Least Functionality

Administrators shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

Network Diagram

Network administrators will maintain a complete topological drawing depicting the interconnectivity of the county's network, systems and services. The network topological drawing shall include the following:

- All communications paths, circuits, and other components on the network.
- The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
- "For Official Use Only" or "Confidential" markings.
- The date (day, month, and year) the drawing was created or updated.

Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Administrators shall protect the system documentation from unauthorized access consistent with the provisions described in Access Control <link>.

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**:

- Configuration management involves the practice of processing system changes systematically with the primary intent of updating the system while maintaining system integrity. A good CM program implements detailed policies, procedures, and techniques while employing the proper CM tools necessary to manage revisions, track revision status, and document and verify each step throughout the process.

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 configuration of county technology resources.
2. Designate an individual or individuals responsible for configuring any technology not supported by Information Services.

Information Services

1. Develop and implement configuration management standards and processes, including system hardening requirements all Ramsey County information technology assets.
2. Oversee approved/unapproved devices via certificates or safe/white listing
3. Routinely assess compliance with configuration management policies and standards.
4. Report on information system vulnerabilities.

Designated support teams (Information Services and business)

Ramsey County has a distributed technology infrastructure support model. The following groups are responsible for managing system configurations 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 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 maintain Ramsey County applications and services.
- Vendors manage a variety of 3rd party-supported technologies, including servers, desktops, peripherals, and networks.

Each of the above-reference support teams will:

1. Ensure that all technologies supporting department applications are configured in accordance with this policy and related standards.
2. Ensure configuration management processes and procedures are followed for department-owned or supported information technology assets.
3. Identify and correct information system vulnerabilities.
4. Report information system security vulnerabilities to Information Services security team.

Application Owners

1. Work with the responsible infrastructure support team to ensure that all technologies supporting their applications are patched in accordance with policy.
2. Test the applications after patch installation for effectiveness and potential side effects on Ramsey County software before deployment to production.
3. Incorporate infrastructure-related flaws remediation and patch management into its configuration and change management process.
4. Provide shutdown and restart procedures for applications that require special handling or care.

PROCEDURES

1. Designated support teams report known system security or compliance weaknesses or vulnerabilities to the IS security team through the **IS Service desk**, 651-266-3452.
2. Designated support teams establish department-specific processes and procedures for configuration management in accordance with this policy and related standards.

LINKS AND RESOURCES

- Ramsey County Configuration Management Standard (link pending): This document lists the specific actions and devices to enforce this policy.

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
Nov. 13, 2020	Initial Draft

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, Nov. 13, 2020
Revision History Date Monday, February 1, 2021

IT Hardware-Software Standard

‹ Patch Management Standard Back IT Hardware-Software Standard ›