Policy Title Patch Management Policy
Department Information Services
Chapter 5
Section 8
Policy 1
Effective Date Monday, August 19, 2019

POLICY STATEMENT

All Ramsey County information technology system components and software must be properly patched with the most current updates and security patches within the timelines associated with their risk and severity score. Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing, and verifying.

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.

Patch management is not specifically mentioned in the 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

Ramsey County is committed to and responsible for ensuring the confidentiality, integrity and availability of the data and information stored in its systems. Patch and vulnerability management is a best practice designed to prevent exploitation of IT vulnerabilities that may exist within an organization. Patches can address vulnerabilities that could be exploited by hackers, fix problems or add new functionality to an existing program. They are provided by a vendor or developer in response to functional or code improvements, flaw or interoperability issues or version/feature updates. Timely patching of known security issues is critical in protecting county systems and data.

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 located in the **Information Services Data Dictionary**:

- Configuration management.
- Information technology.
- Internet of Things (IoT).
- Non-security related patch.
- Patch management.
- Security related patch.

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

Information Services

1. Develop and implement patch management standards and processes, including patch deployment requirements and minimum patching levels for all Ramsey County information technology assets.
2. Designate a maintenance window(s) for patches to be completed for information technology assets supported by Information Services.
3. Routinely assess compliance with patch 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 patch deployments 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-reference support teams will:

1. Ensure that all technologies supporting department applications are patched in accordance with this policy and related standards.
2. Ensure patch 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.
5. Replace hardware and software that can no longer be supported or patched.

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**, 266-3452.
2. Designated support teams establish department-specific processes and procedures for patch management in accordance with this policy and related standards.

LINKS AND RESOURCES

- **Ramsey County Patch Management Standard**
- **NIST National Vulnerability Database**

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
12/7/2020	Updated this policy to include more detail around applicability and responsibilities. Reviewed by Rich Christensen, Eric Brown and Chris Bogut.
8/19/2019	Original Policy

APPROVAL

Rich Christensen
Ramsey County Chief Information Officer
Nov. 13, 2020
Revision History Date Monday, August 19, 2019

Patch Management Standard