Policy Title Malware Protection Policy
Department Information Services
Chapter 5
Section 8
Policy 8
Effective Date Saturday, February 13, 2021

POLICY STATEMENT

Ramsey County is responsible for securing its workstations, laptops, and servers that contain or transport data for county residents. Inherent in this responsibility is an obligation to protect against malware, such as viruses and spyware. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

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 Information Services, application owner and support model.

GENERAL INFORMATION

GENERAL ANTI-MALWARE

- All workstations, laptops, and servers with access to Ramsey County data or networks must have an antimalware application installed that offers real-time scanning protection to files and applications running on that system. This application must protect against viruses, spyware, worms, ransomware, and related risks. Device users will not have the ability to:
  - Disable or bypass malware protection
  - Alter the settings for malware protection in a manner that reduces its effectiveness
  - Alter the frequency of antimalware updates
- Any threat that is not automatically cleaned, quarantined, and subsequently deleted by malware protection software constitutes a security incident and must be reported to the IS Service Desk.
- Antivirus/antimalware signature updates shall occur on a frequency defined by Information Services but not less than once each calendar day.
- Antivirus software will be updated to the latest binaries as they become available.

MAIL SERVER ANTI-MALWARE

If the target system is a mail server, it must have either an external or internal antivirus scanning application that scans all mail to and from the mail server. Local antivirus scanning applications may be disabled during backups if an external antivirus application still scans inbound emails while the backup is being performed.

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

- Virus: a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code.
- Spyware: software that aims to gather information about a person or organization and send such information to another entity in a way that harms the user.
- Worm: a standalone malware computer program that replicates itself to spread to other computers.
- Ransomware: a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

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 protection from malicious software.

Information Services

1. Develop and implement malware protection standards and processes to support this policy and configure antimalware applications accordingly.
2. Assess and respond to malware threats as defined in incident management policies and procedures.

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 a subset of 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 Windows devices supporting department applications run malware protection as required by this policy.
2. Report any malware threats to the Information Services security team at **ISSecurity-DL@co.ramsey.mn.us**.

LINKS AND RESOURCES

- **Mobile Device Security & Use Standards**: Outlines the conditions by which mobile devices are allowed to connect to the Ramsey County network and includes requirements for antimalware on these devices.

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
February 13, 2021	Original Policy

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, Feb 13, 2021
Revision History Date Tuesday, February 23, 2021