Policy Title Network Security Policy
Department Information Services
Chapter 5
Section 8
Policy 9
Effective Date Friday, July 23, 2021

POLICY STATEMENT

This policy outlines the general, high level rules that apply to Ramsey County's network infrastructure to ensure the availability, integrity, and confidentiality of the data on that network. The rules below, when implemented as part of a broader security effort, will protect Ramsey County from a variety of threats, both inside and outside the network.

APPLICABILITY

This policy applies to the LAN and WAN, and any remote connections into the county's environment, such as VPN. All components of these networks are included, such as switches, routers, firewalls, and Internet of Things (IOT devices). This policy is relevant to Criminal Justice Information Services (CJIS), Health Insurance & Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI-DSS).

GENERAL INFORMATION

Separation of networks

Networks will be physically or logically separated according to trust levels:

- Servers and their services/applications that are exposed to the Internet will exist on a DMZ. The DMZ will be isolated by a security gateway, such as a firewall, that filters traffic between the DMZ and LAN. The DMZ will be isolated by a security gateway, such as a firewall, that filters traffic between the DMZ and the internet.
- As needed, visitors will have access only to a separate network that has no path to Ramsey County systems.

Account access control

Network devices will adhere to the **Ramsey County Access Control Policy**, **Privileged Access Policy**, and the **Ramsey County Password Standard**, with particular attention paid to the following areas:

- Network devices may not use default passwords.
- Passwords must adhere to the password standard for complexity requirements.
- The enable/administrative password must always be kept in a secure, encrypted form.

Device configuration

Network devices will adhere to the **Ramsey County Configuration Management Policy**, the **Ramsey County Patch Management Policy**, and these additional parameters:

- Devices must be configured to resist denial-of-service and man-in-the-middle attacks. These configurations may include disabling directed IP broadcasts and disabling TCP/UDP small services, in addition to employing an intrusion prevention system.
- Devices will not utilize telnet, FTP, and HTTP services but may use their encrypted counterparts (i.e., SSH, SFTP, and HTTPS).
- Devices will have source routing and switching disabled.
- All routing updates shall be done using secure routing updates. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
- Devices will drop external packets from invalid sources such as RFC1918 addresses.
- All web services running on router discovery protocol on Internet connected interfaces will be disabled.
- Discovery protocols, dynamic trunking, and scripting environments will be disabled.
- NTP will be configured to a standard, corporate source.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- Access control lists for transiting the device are to be added as business needs arise.
- SNMP traffic is restricted to SNMP collectors.
- Use Ramsey County-standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems but will be at least version 2c.
- Critical network devices, such as core routers and switches, will be fault tolerant, either by internal redundancies or via multiple devices configured for high availability.
- Critical communication links will be redundant and configured for automatic failover.
- Firewalls will be configured as fail safe so that the loss of firewall(s) will not allow traffic to pass unfiltered.

Network alarms and logging

- Critical network components and communication links will be monitored for failure. A loss of any critical component, whether highly available or not, will generate an alarm that will inform Information Services. Such alarms will be generated as quickly as possible, while allowing sufficient time to screen for false alarms.
- All administrative/privileged access will be logged, preferably on a device other than the one being monitored. This means that the logs themselves should be written to a second device so that they can be recovered and reviewed if the network device is destroyed or tampered with. Regardless of where the logs are written, they will periodically be reviewed for any irregularities and for proper account access.

Remote access

- Remote access into the environment will require identification and authorization.
- Site-to-site IPSec VPN tunnels will minimally be configured with IKEv1 SHA1 AES128 ESP encryption with pre-shared keys communicated by voice (not email). Keys will include 1 capital letter, optionally 1 number, and if supported, 1 special character. Minimum length is 8 characters. This is the minimum configuration and may be exceeded.
- All access will be logged, and those logs will be kept on a device other than the communication endpoints.

Configuration auditing

- Network devices will be reviewed annually for adherence to these policies. Any deviation will be documented via CIO signed policy exception and remediated in accordance with change policies.

Wireless access

Network devices will be compliant with Ramsey County's Mobile and Wireless Device Security Policy <reviewing this the week of 7/19. Will add the link once available>, with particular attention paid to these areas:

- All wireless networks controlled by Ramsey County will be secured with strong encryption and a key that cannot be easily intercepted. At the time of writing, this includes WPA-2, but as technologies evolve, other methods may be employed that offer equal or greater protection against current threats.
- Wireless networks will use an encryption key that adheres to the password policy complexity requirements.
- Clients may not attach to the wireless network without the encryption key.

Firewall configuration

- Firewalls are required where Ramsey County's network interfaces with an untrusted network, such as the Internet.
- Firewalls will be capable of next gen capabilities, including:
  - Standard firewall capabilities like stateful inspection
  - Integrated intrusion prevention
  - Application awareness to see and block risky applications
  - Threat intelligence sources
  - Upgrade paths to include future information feeds
  - Techniques to address evolving security threats

DNS

- Internal names will be available only for internal resolution. External parties may not resolve internal names.
- Publicly available DNS servers will be authoritative and not recursive.
- DNS services will be isolated from DNS resolution.
- Any server that hosts the master copy of any zone will be set as a hidden primary. End users will not be permitted to send and receive information from these servers. They exist only to serve secondary name servers.

Remote Site Networks

Remote and satellite sites with their own ISP connections, such as Comcast Business Class ISP connections or similar, may not meet all aspects of this network policy. In such instances, these sites will be separated from Ramsey County's internal network via a firewall.

AUTHORITY

This policy was prepared under the authority of the County Manager, as delegated to the Ramsey County Chief Information Officer. Failure to comply with this policy may result in the suspension of use and connectivity privileges. It may also result in disciplinary action, up to and including termination of employment.

DEFINITIONS

Network: Within this policy, the *network* is defined narrowly as the transport medium that facilitates electronic communication among many computers.

Denial of Service Attack: a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests to overload systems and prevent some or all legitimate requests from being fulfilled. Well-known examples include Smurf, Fraggle, SYN, and Teardrop.

Man-in-the-Middle Attack: an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Eavesdropping is one example of such an attack and can be accomplished by hijacking a wireless connection or tapping into wired ones.

RESPONSIBILITIES

Ramsey County

1. Ramsey County reserves the right to refuse the ability to connect to county resources.
2. Ramsey County will investigate violations as needed to protect its data and resources.

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.
- Information Security will be the sole approver for all external network interfaces.
- Information Security/CIO 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.
- 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 with network management responsibilities will:

1. Develop and implement network security standards and processes.
2. Refer expected violations of County information technology policies and any vulnerabilities in County information systems to Information Security at **ISSecurity-DL@co.ramsey.mn.us**.

LINKS AND RESOURCES

- **Access Control Policy**: Describes how access to systems and data will be restricted to authorized personnel.
- **Privileged Access Policy**: Describes how administrative access to systems and data will be restricted to authorized personnel.
- **Configuration Management Policy**: Governs how information technology system components and software are configured and hardened to minimize vulnerabilities.
- Mobile and Wireless Device Security Policy (in review)
- **Patch Management Policy**: Governs how information technology system components and software are patched with the most current updates and security patches within the timelines associated with their risk and severity score.
- **Password Standard**: Describes minimum requirements that apply to authenticators used to access all Ramsey County systems and data.

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
July 19, 2021	Initial version.

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, July 19, 2021
Revision History Date Friday, July 23, 2021

Wireless Access Device Security Standard

‹ Malware Protection Policy   Back   Wireless Access Device Security Standard ›