Policy Title Bring Your Own Device Policy
Department Information Services
Chapter 5
Section 4
Policy 3
Effective Date Wednesday, February 3, 2021

POLICY STATEMENT

Privately owned mobile devices, desktops, and laptops may connect to the Ramsey County network and systems if they meet county standards. County employees will follow all requirements, policies, standards, and procedures related to approval, acquisition, use and security of such devices. Privately owned technology is not supported by Ramsey County Information Services.

APPLICABILITY

This policy applies to all Ramsey County employees, which for the purposes of this policy includes interns, consultants, contractors, and elected and appointed officials with access to Ramsey County information technology resources. It covers mobile devices, desktops, and laptops not issued or managed by Ramsey County.

This policy is relevant to Criminal Justice Information Services (CJIS) section 5.5.6.1 (Personally Owned Information Systems) and is generally relevant to the Health Insurance & Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI-DSS) where employee-owned devices are involved.

GENERAL INFORMATION

It is the responsibility of Ramsey County employees and elected officials to ensure that county data and resources are protected from loss and unauthorized access. The county is also accountable to the taxpayer for the cost-effective and efficient use of county resources. Use of mobile devices provides opportunities for efficiencies in our work, but it also introduces risk. The Department of Information Services (IS) maintains a list of standards and minimum-security requirements for mobile devices connected to county resources (see **Mobile Device Security and Use Standards**). IS will update these requirements as needed to address security needs or changes in technology.

Rules govern the storage and transmission of regulated information, such as Electronic Protected Health Information (ePHI), Criminal Justice Information (CJI), Payment Card Industry (PCI), and Personally Identifiable Information (PII). This data may not be stored on employee-owned devices without a written business case that explains why such storage is necessary and the business case is approved by the employee's department head, Information Security and the Compliance and Ethics Office. If an employee is using a personally owned device or a county owned mobile device to access CJI, then the device must be enrolled in the county's mobile device management. If regulated information is accessed from an employee-owned device, then that access must be secured per Ramsey County policy. Employees may not print this data on printers that Ramsey County does not own.

With Information Services permission, users are permitted to connect their own monitors, keyboards, and mice to county-owned desktops and laptops, but they may not connect their own storage devices or printers or any devices requiring the installation of software device drivers. These types of devices present security and stability risks.

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

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

- Mobile Device: Electronic handheld device such as a Smartphone or tablet that provides access to Ramsey County resources such as e-mail, calendars, contacts, as well as other applications, without being connected to the Ramsey County network via a physical network connection. This includes Smartphones, Blackberries, and tablet devices (such as the iPad); this does not include simple cell phones that lack the capability to connect to County resources, or laptops and desktop systems.
- Mobile Device Service Plan Allowance: An allowance paid to the employee to offset the cost of the business use of a voice or voice/data plan and related service on an Employee-Owned Mobile Device or cell phone, should a service plan be required for business use.
- County-owned Mobile Device: A device purchased and maintained by the County. The type of device and service plans purchased must adhere to County standards. Information on standard devices is included in the Mobile Device Implementation Guidelines. The device must be able to meet security requirements for connecting to County resources.
- Employee-owned Mobile Device: A device purchased and maintained by the employee who has been approved for access to County resources by the employee's department. The employee chooses the type of device and service plan, if a voice or voice/data plan is desired, but the device must be able to meet security requirements for connecting to County resources.

RESPONSIBILITIES

Ramsey County

1. Ramsey County is not obligated to provide office peripherals, such as printers and monitors, to employees who are working remotely.
2. Ramsey County is not liable for damages caused by inappropriate use of mobile and remote devices.
3. Ramsey County reserves the right to refuse the ability to connect to county resources.
4. Ramsey County will investigate violations as needed to protect its data and resources.

Departments

1. Review remote working requests from their employees and approve or reject these requests as appropriate. Determine business needs for approval of county-owned or employee-owned remote computing devices. Departments will determine whether an allowance will be authorized for an employee-owned device.
2. Annually review mobile/remote device allowances within the department and determine continuation.
3. Understand which of their employees are working from a mobile device or from a personally owned computer. Understand the nature of work their employees are performing from these devices.
4. 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**.

Users of employee-owned and mobile devices

1. Comply with the policies, standards, and procedures listed in the Links and Resources section below.
2. Ensure reasonable physical security for the devices being used.
3. Use devices in a safe manner and comply with applicable policies and laws regarding safe use.
4. Non-exempt employees will comply with employee policies and rules related to work hours.

LINKS AND RESOURCES

- **Mobile Device Acquisition & Activation Procedures**: A guide to authorizing, acquiring, and activating a mobile device.
- **Mobile Device Security & Use Standards:** Governs how mobile and remote devices need to be configured and secured.
- **Secure Data Transmission Policy**: Governs the security of information over a network.
- **Acceptable Use Policy:** Stipulates how devices should and should not be used when conducting business for the County.
- **Ramsey County Data Privacy Policies:** A list of policies that govern how sensitives, confidential, and regulated data should be handled.
- **Cloud and Removable Media Policy**: Specifies the conditions by which information may be stored on removable media or in the cloud.

CONTACTS / SUBJECT MATTER EXPERTS

- **Ramsey County Chief Information Security Officer**
- Ramsey County Chief Compliance and Ethics Officer

Date	Brief description of change
June 21, 2021	Clarified the supportability of privately owned devices in the Policy Statement. Clarified what peripherals users may connect to county-owned devices in General Information. Reapproved by Rich Christensen.
Feb. 3, 2021	Initial version.

APPROVAL

- Rich Christensen, Ramsey County Chief Information Officer, Feb. 3, 2021
- Deanna Pesik, Chief Compliance and Ethics Officer, Feb. 3, 2021

Revision History Date Tuesday, February 9, 2021