Policy Title Access Control Policy
Department Information Services
Chapter 5
Section 2
Policy 1
Effective Date Tuesday, November 18, 2014

POLICY STATEMENT

Ramsey County will maintain access control policies and standards that minimize risk while maximizing protection of Ramsey County technology resources and data. Only properly identified, authenticated, and authorized users will gain access to Ramsey County systems and data required to perform their role.

All Ramsey County information systems must employ access controls to restrict read, write, execute, and other privileges to authorized personnel. Users must be positively identified and authenticated in accordance with this policy before access to information, networks, or systems is granted.

APPLICABILITY

This policy is applicable to all individuals, paid or unpaid, who work on behalf of Ramsey County. This policy is relevant to Criminal Justice Information Services (CJIS) section 5.5 (Access Control) and section 5.6 (Identification & Authentication) as well as the Health Insurance Portability and Accountability Act (HIPAA) sections 164.308(a)(3) and 164.308(a)(4).

GENERAL INFORMATION

This policy governs user access to Ramsey County data and technology resources by requiring adequate controls for identification, authentication, authorization, and auditing.

- Identification: Anyone seeking access to Ramsey County technology resources will be required to identify themselves with a unique credential.
- Authentication: Identification will be verified via an authentication mechanism that provides reasonable proof of identity.
- Authorization: After the identity is authenticated, the user will be authorized to perform pre-approved actions on the system to which they have authenticated.
- Auditing: User actions on these systems will be logged for future reference and auditing.

The four broad controls summarized above are enforced via the mechanisms below.

User Identification

Each person who is authorized to store, process, and/or transmit sensitive information shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access sensitive information or networks leveraged for its transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. User IDs may not give any indication of the user's privilege level (for example, administrator, manager, or supervisor). Systems shall require users to identify themselves uniquely before the user is allowed to perform any actions on them. Administrators shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

Password

When administrators use a password as an authenticator for an individual's unique ID, they shall adhere to the **password standard**.

Account Management

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations.

Administrators shall grant access to the information system based on:

- Valid need-to-know that is determined by assigned official duties.
- Satisfaction of all personnel security criteria.

The administrator responsible for account creation shall be notified when:

- A user's information system usage or need-to-know status changes.
- A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.
- The account has not been accessed for 90 consecutive days. Inactive accounts will be disabled or removed unless an exception is granted.

Administrators shall validate information system accounts at least annually and shall document the validation process. The validation process will confirm compliance with the rules contained herein.

Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. See **privileged access control policy**.

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed to control access between users and objects in the information system.

Least Privilege

Administrators shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. Users must not use their access control rights for anything that exceeds the purpose for which the rights were originally granted. Ramsey County Information Services retains the discretion to make its own minimum necessary determination when access is requested to protected information.

System Access Control

Access control mechanisms to enable access to sensitive information shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

- Prevent multiple concurrent active sessions for single users for applications accessing sensitive information unless there is a documented operational business need.
- Ensure that only authorized personnel can add, change, or remove component devices, dialup connections, and remove or alter programs.

Access Control Criteria

Administrators shall control access to electronic information based on one or more of the following:

- Job assignment or function (i.e., the role) of the user seeking access.
- Physical location.
- Logical location.
- Network addresses (e.g., users from sites within a given department may be permitted greater access than those from outside).
- Time-of-day and day-of-week/month restrictions.

Access Control Mechanisms

When setting up access controls, administrators shall use one or more of the following mechanisms:

- Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object and the types of access they have been permitted.
- Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
- Encryption. Encrypted information can be decrypted, and therefore read, only by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management.
- Geofencing. Administrators will block access from outside the United States. See remote access, below.
- Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the county.

System Use Notification

The information system shall display an approved system use notification message before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

- The user is accessing a restricted information system.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
- Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

- The system use information is available and when appropriate, is displayed before granting access
- Any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities
- The notice given to public users of the information system includes a description of the authorized uses of the system.

Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session

lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications used within physically secure facilities that remain staffed when in operation, are exempt from this requirement. An example of a session lock is a screen saver with password.

Remote Access

Administrators shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to a Ramsey County information system by a user or an information system communicating temporarily through an external, non-county-controlled network (e.g., the Internet).

Administrators shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. Administrators shall control all remote accesses through managed access control points. They may permit remote access for privileged functions only for compelling operational needs and shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Access to Ramsey County resources from outside the US is restricted to web-based Office 365 resources only, such as Outlook, Teams, etc. Obtaining this access requires submission of the **Out of Country Login Request** form, which the user's manager and IS Security must approve before access is granted. Taking a Ramsey County laptop out of the U.S. is strictly prohibited unless on county business and requires approval by the Chief Information Security Officer (CISO).

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

- An authorized escort shall always monitor the session.
- The escort shall be familiar with the system/area in which the work is being performed.
- The escort shall have the ability to end the session at any time.
- The remote administrative personnel connection shall be encrypted to a level of security meeting or exceeding Federal Information Processing Standards (FIPS) 140-2.
- The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This may be accomplished via electronic authentication protocols or during the session via active teleconference with the escort.

Personally Owned Information Systems

A personally owned/non-county device is permitted to access the Ramsey County network if it meets the conditions identified in the **Bring Your Own Device Policy**. This control does not apply to the use of personally owned information systems to access the county's information systems and information that are intended for public access (e.g., a public website that contains purely public information).

Publicly Accessible Computers

Ramsey County employees will not access, process, store, or transmit sensitive Ramsey County information on untrusted devices, such as publicly accessible computers. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, and public kiosk computers.

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 loss of access privileges and disciplinary action, up to and including termination of employment. Violations of local, state or federal law are subject to potential prosecution in those jurisdictions.

DEFINITIONS

- Access: The level and the extent of permissions to systems and data a user is granted to accomplish the intended purpose of any program, request task or service.
- Authentication: A method of verifying a user's identity, for example through use of a password.
- Identification: The means by which a system user is recognized, for example by logging in to the network.
- Identity: Information about the user that distinguishes them as an individual and verifies their status within the County. The identity of a user is unique to that user.
- Sensitive Data: Information that, if improperly disclosed, could lead to legal, financial, and reputational risk to Ramsey County.
- Users: Any Ramsey County employee or contractor authorized to access Ramsey County Information Technology resources, regardless of role.

RESPONSIBILITIES

Ramsey County

1. Ensure the security of its data, systems, and users' accounts.
2. Investigate violations as needed or directed to protect its data and resources or to provide information relevant to an investigation.

Departments

1. Complete an annual attestation of compliance with access control policies, standards, guidelines and procedures, including review and reporting requirements.
2. Investigate alleged violations of Ramsey County information technology policies. Report any known weakness or vulnerability in Ramsey County information system security or compliance as outlined in procedures.

3. Managers must request access changes when a person's job responsibilities change resulting from hiring, transferring, change of assignment, placing on investigatory leave or terminating employment.

Application Owners

1. Designate an individual or individuals responsible for access control for each business application to ensure policies and standards are enforced, and users are granted access only to systems and information required to perform their jobs.
2. Develop and adhere to access control procedures for each application the business supports.

Designated support teams (Information Services and business)

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

Users

1. Understand and comply with county policies, standards, guidelines, and procedures governing access to county information and technology resources.
2. Complete the mandatory annual Ramsey County information security training.

LINKS AND RESOURCES

- **Password Standard**: Details the rules governing construction and maintenance of passwords used to access Ramsey County technology systems.
- **MFA Standard**: Specifies the mechanisms that govern secondary authentication controls, such as soft tokens and hard tokens.
- **Bring Your Own Device Policy**: Identifies the conditions by which employee-owned devices are permitted to connect to the Ramsey County network.
- **Mobile Device Policy**: Governs the configuration of devices that connect to the Ramsey County network remotely from an untrusted network or wirelessly from any network.
- **Ramsey County Out of Country Login Request**: The form to use to request permission to login to Ramsey County from outside the United States.

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
8/1/2022	Clarified language for accessing Ramsey County resources from outside the United States.
6/3/2022	Added policies for out-of-country access.
4/18/2022	Merged components of the access control standard with this policy. Added a sentence to reference access from outside the U.S.
1/18/2021	Added sections for account management, access enforcement, least privilege, system access control, access control criteria, access control mechanisms, unsuccessful login attempts, system use notification, session lock, remote access, personally owned information systems, publicly accessible computers, identification policy and procedures, and password. Added definitions, updated responsibilities, and identified HIPAA and CJIS applicability.
2/5/2020	Rewrote this policy to simplify language, remove obsolete terms and better define responsible individuals and departments.
11/18/2014	Initial version.

APPROVAL

Chetan Ganatra
Ramsey County Chief Information Officer
April 18, 2022

Multifactor Authentication Standard

Password Standard

Security Exception Procedure

Vendor Remote Access Standard