Policy Title Privileged Access Policy
Department Information Services
Chapter 5
Section 2
Policy 2
Effective Date Friday, December 4, 2020

POLICY STATEMENT

Ramsey County will maintain stringent access controls around privileged/administrative accounts to minimize risk to and maximize protection of Ramsey County technology resources and data. Only properly identified, authenticated, and authorized personnel will be granted administrative access to Ramsey County resources, and their access will be periodically reviewed for appropriateness and adherence to rules governing the security of Ramsey County data and systems.

APPLICABILITY

In addition to domain accounts, this policy is applicable to users, internal and external, with administrative, supervisory, root, elevated, or privileged access to any other computers, applications, or databases that maintain data hosted by or on behalf of Ramsey County. Accounts to which this policy applies include:

- Administrative domain accounts for named users (a.accounts, az.accounts, bt.accounts, f.accounts, o.accounts, and t.accounts)
- Named domain accounts with privileged access to domain applications or systems
- Domain service accounts
- Domain system/application accounts
- Domain accounts with privileged access to servers
- Local server accounts with privileged access
- Non-domain accounts with privileged access to internal or external systems

GENERAL INFORMATION

Ramsey County access control policies are designed to provide access to the minimum necessary information required to perform work while preserving the security and integrity of Ramsey County data and technology resources. Access control involves managing who has access to specific systems and resources at a given time. This is accomplished through identification, authentication, and authorization.

This policy regulates access to Ramsey County's systems and information assets and preserves the fundamental information security principles of confidentiality, integrity, availability, accountability, and assurance. This includes maintaining secured systems and networks.

AUTHORITY

This policy and the procedures herein were prepared under the authority of the County Manager, as delegated to the Ramsey County Chief Information Officer.

DEFINITIONS

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

- Access
- Authentication
- Covered Individuals
- Identification
- Identity
- Information
- Privileged Access
- Users

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 privileged 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.

Application Owners

1. Policy Compliance: Grant privileged access to Ramsey County information and technology resources in a manner consistent with access policies and standards. Develop and adhere to privileged access control procedures for each application the business supports.
2. Access Review: Review privileged access accounts annually to determine if privileged access is still needed and to review what level of access is appropriate for each person or role. Ensure that privileged access users are granted access only to systems and information required to perform their jobs.
3. Unique User Accounts: Privileged access users must use individual accounts with unique usernames and passwords that comply with the county password policy. If there is a business need for shared credentials, an approved password storage system must be used. Access to the password storage system must be controlled by the county's approved multi-factor authentication.
4. Obsolescence: Privileged accounts shall be disabled or deleted when the tasks for which the accounts were created are no longer required or when the accounts have been inactive for 90 days.
5. Least Privilege: Follow the principle of least privilege when allocating privileged accounts. Privileged access users must have their access set to the lowest level of access needed to accomplish their job function. Moreover, such users will invoke their privileged accounts only for tasks that require it. If means other than privileged access will accomplish a task, then those other methods must be used.
6. Auditing: Maintain access logs in a centralized system where integrity and access can be controlled. IS will have access to review those logs as needed to monitor privileged access user accounts for misuse. The type of logs and the frequency of log review are to be determined based on the data classification and data types contained in the system. System/data owners must follow federal and state regulations and county policy in developing their log management and review procedures.

Designated support teams (Information Services and business)

Ramsey County has a distributed technology infrastructure support model. The following groups are responsible for managing privileged access control 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 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 manage applications and business 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 adhere to all the rules outlined for application owners above and will apply these same rules to systems, applications, and platforms that the support team maintains:

- Policy Compliance
- Access Review
- Unique User Accounts
- Obsolescence
- Least Privilege
- Auditing

LINKS AND RESOURCES

- **Access Control Policy**
- Access Control Standard (under review)
- **Password Standard**
- Privileged Access Standard

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County Chief Information Security Officer

REVISION HISTORY

Date	Brief description of change
Nov. 17, 2020	Initial version. Reviewed by Chris Bogut, Eric Brown, Rich Christensen.

APPROVAL

Rich Christensen, Ramsey County Chief Information Officer, November 17, 2020
Revision History Date Friday, December 4, 2020

Privileged Access Standard

‹ Vendor Remote Access Standard

Back

Privileged Access Standard ›