Policy Title Criminal Justice Information Handling Policy
Department Information Services
Chapter 5
Section 3
Policy 1
Effective Date Monday, November 10, 2014

Jump to forms

POLICY STATEMENT

Ramsey County will apply all necessary and reasonable protection to the handling and storage of Criminal Justice Information (CJI), regardless of form, to protect against unauthorized disclosure, alteration, or misuse.

APPLICABILITY

This policy is applicable to all covered individuals and to any others, paid or unpaid, who do work on behalf of the county, and have or may have direct access to CJI. Any person who is found to have negligently violated policy may be subject to disciplinary action, up to and including termination of employment. Violations that may involve illegal activity may be referred to law enforcement and/or reported to other authorities as required by law. When multiple policy statements or security standards apply to a specific situation, the most restrictive security standards will apply.

GENERAL INFORMATION

Ramsey County uses the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS), the world's largest repository of criminal fingerprints and history records, to protect its citizens while preserving their civil liberties. As such, federal and state government policies require certain controls over the storage, handling and transfer of data.

AUTHORITY

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

DEFINITIONS

Please refer to the **FBI CJIS Security Policy - Appendix A** and the **Bureau of Criminal Apprehension (BCA) Criminal Justice Data Communications Network (CJDN) Security Policy 5002** for the following definitions:

- Criminal Justice Information
- Criminal Justice Information Services
- Direct Access

RESPONSIBILITIES

Departments

1. Assess and enforce their employees' compliance with policy and investigate non-compliance.
2. Obtain and file completed CJI Handling User Agreement and make available for review when requested.

Information Services

Review Information Security and technology policies, standards, guidelines and procedures periodically or when significant changes are implemented and update them as needed.

Users

1. Shall **NOT** send CJI via electronic mail.
2. Shall **NOT** use cloud or internet-based hosting services to store or share CJI.
3. Shall comply with any additional security policies, procedures, and practices established by departments with access to CJI.
4. Complete a mandatory user agreement of compliance with this policy.

PROCEDURES

None.

LINKS AND RESOURCES

- **FBI CJIS Security Policy (http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center)**
- **CJI Handling User Agreement** (Word)

CONTACTS / SUBJECT MATTER EXPERTS

REVISION HISTORY

Date	Brief description of change

APPROVAL

Johanna M. Berg
Chief Information Officer
November 10, 2014