140. Criminal Justice Data Communications Network (CJDN) Security & Criminal Justice Information Services (CJIS) Policy

RICHFIELD POLICE DEPARTMENT POLICY

Effective Date:	03/01/11
No. of Pages:	4
Serial Number:	10-040
Authority:	Chief Jay Henthorne

NOTE: This policy is for internal use only and does not enlarge an employee's civil or criminal liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this policy, if proven, can only form the basis of a complaint by this Department, and then only in a non-judicial administrative setting.

I. PURPOSE

The purpose of this Policy is to establish proper procedures when using the Criminal Justice Data Communications Network (CJDN) and Criminal Justice Information Services (CJIS).

The Richfield Police Department is committed to maintaining a high degree of information security for its protected CJIS Environment. In order to accomplish this, the Richfield Police Department has adopted all of the core security controls outlined in the FBI's CJIS Security Policy Version 5.8 (and future versions). The CJIS 5.8 (and future versions) Security Policy manual is located on the RPDNet Intranet internal website.

All Richfield Police Department staff, as well as any non-criminal justice contractor(s) and personnel, shall follow the security controls as outlined in the CJIS Security Policy Version 5.8 (and future versions).

Specific CJIS policy-mandated procedures (CJIS Security Addendum) that accompany this policy can be found on the RPDNet Intranet internal website.

II. POLICY

This policy shall be considered the official CJDN/CJIS Security Policy for the Richfield Police Department, regarding the physical and personnel security of the CJDN system and CJIS data. All staff must follow the policies contained herein. This will assure proper usage of the system and adherence to all local, state, and federal regulations that govern the use of the MNJIS computer system. The Terminal Agency Coordinator (TAC) for Richfield Police Department is the Records Supervisor. The TAC manages the operation of the CJDN terminal on a local agency level and is responsible for ensuring that all state and local policies are enforced regarding the use of the CJDN terminal.

III. DEFINITION

CJDN: The Criminal Justice Data Communications Network is the overall system, which provides criminal justice agencies computer access to data stored on state and national systems.

CJIS: The FBI division responsible for the collection, warehousing, and timely dissemination of relevant criminal justice information to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

IV. PROCEDURE

ACCESS TO CJDN SYSTEM

Access to the CJDN shall be limited to employees who have been certified by the BCA to operate the terminal. Currently, at the Richfield Police Department, this is limited to the TAC and trained records personnel. All other personnel of the Department must make their Criminal Justice inquiries through the authorized records personnel or dispatch.

1) Staff having access to the CJDN system must meet the following requirements:
   a) Be an employee of the Richfield Police Department.
   b) Successfully pass a State and National fingerprint background check.
   c) Pass the Full Access Certification test as required.
   d) Be trained and certified within six month of hire and biennially thereafter.
   e) Complete Basic Security Awareness Training within six months of hire or assignment and biennially thereafter.
2) New employees of the Richfield Police Department shall be fingerprinted within 30 days of employment or assignment and the fingerprint cards shall be sent to the BCA for a background check.
3) A potential new employee of the Richfield Police Department shall have a background check completed before they are hired. When running the criminal history on that person, the Purpose Code of "J" shall be used.
4) Fingerprint cards on CJDN operators are to be kept in a locked drawer by an Administrative Aide. Fingerprint cards of the IT personnel will be kept in their personnel files at the Richfield Police Department.
5) The TAC will issue a unique username and password to authorized users with access to the CJDN and Portal 100. Authorized users will be given a unique password to have access to criminal histories. That Criminal History Password will be changed by the TAC at least every two years. A list of these assigned passwords shall be kept by the TAC in a locked cabinet.
6) Individuals visiting the Police Department that do not meet the security requirements listed above must sign-in, be issued a visitor badge and be escorted at all times while in the Police Department.
7) City Staff that do not meet the security requirements listed above will be required to review and sign the *Security Awareness Agreement/Occasional Unescorted Access* form. This agreement will give them occasional access to the Police Department. This agreement is in effect for two years from the date it is signed. It will be kept on file with the Records Supervisor.

Training of Sworn Officers

In order to comply with the FBI CJIS Security Policy (CSP) and the BCA CJDN Security Policy – 5050, all new sworn personnel will be required to watch the BCA's Security Awareness Training and Mobile Access Training and take the subsequent test within two weeks of hire and biennially (every two years) refreshers thereafter. This will be documented by the Records Supervisor.

Security of Terminal

All CJDN terminals are located in the Richfield Police Department within a physically secure location.

All personnel who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS systems must successfully pass a fingerprint based background check.

Criminal History responses, as well as all other CJDN printouts, will be destroyed when no longer needed. These documents will be shredded at the Police Department

Discipline for Misuses of MNJIS/NCIC/CJIS Systems and Data

Inquiries into the motor vehicle registration, driver license, criminal history or any other file in the MNJIS/NCIC/CJIS systems and data will be performed for criminal justice purposes only.

Any employee misusing information or obtaining information for other than official criminal justice purposes from MNJIS/NCIC/CJIS systems and data will be subject to disciplinary action.

When performing any file inquires or making any entries into MNJIS/NCIC/CJIS systems and data, it is important to remember that the data stored in MNJIS/NCIC/CJIS systems is documented criminal justice information and this information must be protected to ensure correct, legal and efficient dissemination and use. The individual receiving a request for criminal justice information must ensure that the person requesting the information is authorized to receive the data. The stored data in MNJIS/NCIC/CJIS systems is sensitive and should be treated accordingly, and unauthorized request or receipt of MNJIS/NCIC/CJIS data could result in criminal proceedings.

When the Chief or the TAC becomes aware that an employee of the Richfield Police Department is using a CJDN terminal, CJDN terminal generated information, CJDN equipment, or MNJIS/NCIC/CJIS systems and data access not in accordance with Department policies, state polices, or MNJIS/NCIC/CJIS systems and data policies and said problem is not deemed merely operator error, the Chief or his designee, or the TAC shall promptly address the violation.

The Chief or his designee shall meet with the person who is alleged to have violated the policy and determine appropriate sanctions, which may include any or all of the standard discipline policies currently in place at the Richfield Police Department, including a documented oral reprimand, written reprimand, suspension, or termination. Intentional misuse of MNJIS/NCIC/CJIS systems and data is a serious violation and the BCA will be informed of such violations. If criminal behavior is believed to have occurred, appropriate agencies will be notified for further investigation.

The specific situation in each case of misuse of MNJIS/NCIC/CJIS systems and data will be looked at, with all circumstances considered when determining disciplinary actions. Consideration will be given to the extent of loss or injury to the system, agency, or other person upon release or disclosure of sensitive or classified information to an unauthorized individual. This also includes activities which result in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss by theft of any computer system media including: Chip ROM memory, optical or magnetic storage medium, hardcopy printout, etc.

The TAC, with the Chief's approval, may at any time terminate a staff person's access to the MNJIS/NCIC/CJIS systems and data for any rule violation.

By Order Of:

Chief of Police

MNJIS/NCIC/CJIS SYSTEMS AND DATA DISCIPLINE POLICY FORM

I have read and understand this policy including "DISCIPLINE FOR MISUSES OF MNJIS/NCIC/CJIS SYSTEMS AND DATA" and the affiliated CJIS Security Addendum for the Richfield Police Department. The sign off sheet will be placed in the employees' personnel file.

_____ _____

Signature Date

_____

Printed Name