MINNESOTA DEPARTMENT OF NATURAL RESOURCES

DIVISION OF ENFORCEMENT

DIRECTIVE

DIRECTIVE NUMBER: A-29-24

SUBJECT: Criminal Justice Data Network (CJDN) Policy

EFFECTIVE DATE: 5-22-2024

SPECIAL INSTRUCTIONS: BCA Criminal Justice Data Communications Network (CJDN) Mandatory Policy.

APPENDIX: None

REFERENCE: BCA mandatory policies on CJDN use

DISTRIBUTION: All Staff

NUMBER OF PAGES: 4

This directive is for division use only and does not modify or supersede any law and should not apply to any criminal or civil proceeding except for civil proceedings related to departmental administrative actions. This directive should not be viewed as creating a higher standard of safety or care in any evidentiary sense. Violations of this directive may form the basis for departmental administrative action.

I. PURPOSE

The purpose of this policy is to guide division staff on the access, use, and security requirements of equipment used to access the Criminal Justice Data Communications Network (CJDN)

II. POLICY

This policy shall be considered the official CJDN Security Policy for the division regarding the physical and personnel security of the CJDN system. All individuals must follow the directives contained within. The policy outlines the use requirements of CJDN access and local, state, and federal systems. The Terminal Agency Coordinator (TAC) for the division is the Administrative Manager. The TAC manages the local agency operation of the CJDN and is responsible for ensuring that all state and local policies are enforced regarding the use of the CJDN.

III. DEFINITIONS

A. Criminal Justice Data Communications Network (CJDN): A secure computer network to access federal, state, and out of state files for criminal justice and authorized non-criminal justice purposes.

B. CJDN Terminal: Division computers set up to allow access to the CJDN.

C. Criminal Justice Information (CJI): Data such as driver's license, and vehicle registration info

accessed through the CJDN.

D. Hit: a positive response from the National Crime Information Center (NCIC) in which the person or property queried appears to match the person or property in the response.

E. Terminal Agency Coordinator (TAC): Person assigned to manage the division's compliance with CJDN policies and procedures.

IV ACCESS TO CJDN SYSTEM

A. Access to the CJDN shall be limited to employees who have been certified by the Bureau of Criminal Apprehension (BCA). Currently, this is limited to Conservation Officers and support staff with a need to access CJDN data.

B. Employees using the CJDN system, configure or maintain computer systems or networks, or have access to areas where criminal justice information (CJI) is processed must meet the follow requirements prior to access:

1. Successfully pass a fingerprint-based background check.
   a. If the individual signs a consent form, a local criminal history background check using search reason ***Criminal Justice Employment- Purpose Code J*** may be completed.
   b. Agencies must keep the background check result letter on file and available during an audit.
2. The TAC shall submit a ***MyBCA User Access Form*** to the BCA Service Desk requesting access to the CJDN, indicating what systems the employee requires.
3. The employee must complete Security & Privacy Training and pass a Single Certification exam. The Employee must recertify annually thereafter.
4. If employees require the Portals system, the TAC shall create a Portals account and assign each employee a unique username and password.
5. Additional training is available in person at the BCA or online in nexTEST regarding NCIC/MNJIS applications.

V. SECURITY OF TERMINAL AND DATA

A. The division will ensure only authorized devices are connected to the CJDN.

B. The CJDN terminal(s) and CJI for the division must be processed and stored in a secure area. Only authorized individuals who have completed the above requirements are allowed unescorted access to the terminals.

C. All CJDN printouts will be destroyed when no longer needed. These documents will be shredded either by an agency approved shredder, or by properly vetted document destruction company.

VI. MISUSE OF CJDN

A. Queries of the motor vehicle registration, driver's license, criminal history, or any other file in the BCA/FBI systems shall be performed only for authorized criminal justice purposes.

B. Officers shall not run themselves, other employees, family, or others for personal use or gain in the BCA/FBI systems. Any employee misusing information or obtaining information for other than official criminal justice purposes from the CJDN will be subject to disciplinary action.

C. When performing any file queries or making entries into BCA/FBI systems, officers shall securely store and protect criminal justice information (CJI).

D. Officers shall also ensure authorized dissemination and use. The officer disseminating the CJI shall ensure that the person requesting the information is authorized to receive the data. Unauthorized request or receipt of BCA or FBI data could result in criminal proceedings.

E. When the Director or the Terminal Agency Coordinator (TAC) becomes aware an employee has accessed the CJDN or used CJI obtained from the CJDN in violation of agency, state, or FBI policies, they shall promptly address the violation.

F. The director shall meet with the alleged violator and determine appropriate sanctions according to standard discipline policy, including but not limited to verbal reprimand, written reprimand, suspension, or termination. The BCA must be notified immediately of misuse. If criminal behavior is believed to have occurred, appropriate agencies shall be notified for further investigation.

G. Each case of misuse of the CJDN system will be investigated, with all circumstances considered to determine disciplinary actions. Consideration will be given to the extent of loss or injury to the system, agency, or other persons upon releasing or disclosing sensitive or classified information to an unauthorized individual. Misuse also includes activities that result in unauthorized modification or destruction of system data, loss of computer system access, or loss by theft of any computer system media, including chip ROM memory, optical or magnetic storage medium, hardcopy printout, etc.

H. With the Director's approval, the TAC may terminate an employee's access to the CJDN system for any violation.

VII. HIT CONFIRMATION PROCEDURE

A. Confirm the person or property queried matches the person or property contained in the hit AND is in your employee's presence.

   1. For wanted person hit, the location must be within the extradition limits indicated on the record.

B. Contact State Patrol Dispatch to inform them of the hit and the location of the person or property.

C. State Patrol Dispatch will perform Hit Confirmation on behalf of the officer.

   1. Ensure the person or property remains in your agency's presence until further direction from the jurisdiction entering the NCIC file**.**

By Authority of:

_____

COL Rodmen Smith
Division Director
Division of Enforcement