

**SILVER BAY POLICE DEPARTMENT  
CRIMINAL JUSTICE DATA NETWORK POLICY**

**POLICY #D-1**

---

**I. PURPOSE**

The purpose of this policy is to provide for the physical security of the Silver Bay Police Department's Criminal Justice Data Network (CJDN) terminal and to establish the rules and regulations necessary to ensure for the proper use of, access to, and dissemination of information accessible through this system.

---

**II. POLICY**

It is the policy of the Silver Bay Police Department to provide its employees access to modern technologies such as cellular phones, internet access, email capabilities, facsimile machines, et al to aid them in the performance of their official duties. Accordingly, employees must adhere to specific standards of conduct when utilizing these technologies as established by City of Silver Bay Personnel Policies and this order.

It is further the policy of the Silver Bay Police Department to utilize technologies and information available through the CJDN in the performance of our official duties in accordance with rules and regulations established by the Minnesota Department of Public Safety – Bureau of Criminal Apprehension (DPS-BCA), the Federal Bureau of Investigations National Crime Information Center (FBI-NCIC), and the National Law Enforcement Telecommunications System (NLETS). See the attached remote access network users agreement and the CJIS Security Policy for further reference.

---

**III. COMMENT**

As evidence by review of the attached User Agreements the CJDN is a very large system that serves the needs of thousands of users in the criminal justice field worldwide. Consequently, strict adherence to policies and procedures established by the system proprietors is necessary to prevent disruption of service or improper use of information in the system and disciplinary measures for misuse of the system are severe for both the agency and the individual perpetrator. Any disciplinary action necessary will be done in accordance with the Two Harbors Police Department personnel policy.

---

**IV. DEFINITIONS**

See copies of the attached Users Agreements for technical definitions.

---

## V. PROCEDURES

- A. Physical Security:** The CJDN access terminal will be located in the Silver Bay Police Department records clerk work area. This computer is to be positioned in such a manner that it is not visually accessible to the public. In addition, a computer screen security device shall be attached to allow for added security. No member of the public, including custodial staff or maintenance personnel, shall be allowed in the area of this computer unless escorted by authorized personnel.
- B. Restricted Access:** All CJDN operators shall be trained and certified within six (6) months of hire or assignment. Basic security awareness training shall be required within six (6) months of initial assignment, and biennially thereafter, for all personnel who have access to Criminal Justice Information (CJI). Only authorized employees who have received appropriate training may access the CJDN through the Two Harbors Police Department terminal. Unauthorized access or attempts to access CJDN is not allowed and will result in disciplinary actions up to and including employee dismissal and pursuit of criminal charges. All authorized employees must undergo a criminal background check prior to being granted access to the system. Additionally, all information management system personnel must undergo appropriate criminal background screening prior to working on the system. This screening must include at a minimum a state and national fingerprint based records check.
- C. “Query Only” Status:** The Silver Bay Police Department is currently a “query only” agency. This means we will not be submitting information for inclusion in the CJDN files directly at this time. The Silver Bay Police Department authorized employees will be the only employees able to access and retrieve information from CJDN. The Lake County Sheriff’s Office will continue to be our point of contact for data entry into the CJDN (i.e. stolen vehicles, missing/wanted persons, second party checks, etc.). Access will be through the T-1 lines provided by Lake County.
- D. Property Hot File Records:** A theft report describing the stolen item including the serial number (SER) or owner applied number (OAN) is required prior to the property entry into the hot files. A check of all appropriate sources (i.e. DNR, DVS, APS, etc.) shall be performed and documented in the case file. The Lake County Sheriff’s Office will continue to be our point of contact for data entry into the CJDN.
- E. Hit Confirmation:** In the event a “hit”, which is a positive response from CJIS and/or NCIC in which the person or property inquired about appears to match the person or property contained in the response, is received, it is the inquiring employees immediate responsibility to contact the Lake County Sheriff’s Office and provide them with all pertinent information so they are able to respond to the “hit” received.
- F. Validations:** The TAC will be responsible for all validations received from CJIS and/or NCIC Hot File records. Validation takes place 60-90 days from the date of entry and yearly thereafter. The TAC shall verify the following:
1. Remove all records that are no longer active from the MCJIS/NCIC Hot Files
  2. Compare all records against the current supporting documentation to ensure:
    - a. That the information in each field is accurate.
    - b. That the records contain all available information found in the case files.

3. Remove all records for which corresponding case file documentation cannot be located OR recreate the case file so the Silver Bay Police Department meets NCIC requirements.
4. Update records as needed when:
  - a. NCIC Code changes occur.
  - b. Agency related information, such as extradition limits or hit confirmation, and/or contact information changes.
  - c. New or additional information becomes available.
5. Contacts:
  - a. Wanted Person – consult the court or prosecutor to verify that the warrant is still active and the extradition limits have not changed for all wanted person records. Operator shall run a new criminal history inquiry (QH – PUR/C) to check for additional available identifiers to add to record (i.e. AKA's, DOB's, etc.). ATN field should contain the name of the person validating the record as well as the reason (VALIDATION). Old CCH record shall be removed from the warrant jacket and shredded and new CCH inquiry shall be placed in the warrant jacket.
  - b. Missing Person – consult the complainant to verify that the person is still missing for all missing person records.
  - c. Orders for Protection – contact the courts to verify that the OFP is still active and all of the information is current and correct.
  - d. Stolen Property – contact the owner or insurance company for stolen property validations to verify that the property is still missing. On stolen vehicles, run a new registration to see if the vehicle has been re-registered to an insurance company or possibly in another person's name.
6. All validation attempts should be documented in the case file.

Upon completion of the validation of all records identified in the printouts, the TAC must ensure that the certification letters are signed and returned within the specified time to the Department of Public Safety.

**G. Computerized Criminal History Checks (CCH/III):** The following rules apply on all CCH/III checks:

1. All individuals authorized to obtain CCH checks will be issued a password by the TAC.
2. All CCH/III checks will require, at minimum, an Initial Complaint Report (ICR) be filed.
3. If the person running a CCH check is doing so for another Department employee, they will ensure that the correct purpose code is being used, and that the ATN field contains the name or badge number of the requesting party, and that the entry contains some information indicating the reason for the check, such as a case number, or a word or phrase useful in relating the check to the purpose.
4. The person responsible for the CCH/III will insure that the hard copy is properly disposed of after use unless a specific circumstance exists which must be approved by the TAC. Upon disposal of a CCH/III check, a note will be made in the case file,

or on the ICR in the event there is no case file, stating the date the CCH/III was destroyed. The proper disposal of criminal history information shall consist of either burning or shredding of the document.

5. In the event another authorized person or agency has a need for a criminal history, i.e. City Attorney or County Attorney, a separate transaction should be initiated using that agency's ORI.

- H. Terminal Agency Coordinator (TAC)/Information Security Officer (ISO):** The records clerk of the Silver Bay Police Department will serve as the Silver Bay Police Department TAC and ISO. The Chief of Police and Assistant Chief of Police, however, shall be involved with, and make any final decisions regarding CJDN access, placement, etc.
- I. Reference Manuals and Passwords:** To ensure sufficient security of information related to access of the CJDN, all reference manuals are to be kept in a locked file cabinet designated by the TAC unless in use and passwords and user names issued to certified operators shall not be shared. It is recommended by the DPS-BCA-CJIS Section that individual operators change their Criminal History passwords on an annual basis. The TAC is responsible for keeping a list of agency criminal history passwords. Portal 100 logon passwords must also be changed when prompted by the system.
- J. Dissemination of Information:** Dissemination of criminal history information to persons outside of the law enforcement community without proper authorization may result in severe penalties for the divulging party, the party's employer, and the State of Minnesota. If you do not know that information can be divulged, contact the Chief of Police, Assistant Chief of Police, or the TAC for further guidance. The subject of data in the CJDN is allowed access to the data only after having been positively identified up to and including the use of fingerprints if necessary.

**SILVER BAY POLICE DEPARTMENT  
CRIMINAL JUSTICE DATA NETWORK POLICY**

**POLICY #D-1**

---

**VI. SUPERVISORS SIGNATURES**

---

Cole W. Ernest  
Chief of Police

---

Sergeant

---

**VII. EFFECTIVE DATE:**

---

**VIII. REVISED DATE**

**SILVER BAY POLICE DEPARTMENT  
CRIMINAL JUSTICE DATA NETWORK POLICY**

**POLICY #D-1**

---

**DATE REVIEWED**

**SIGNATURE**