

EFFECTIVE DATE: February 15, 2012

---

SUBJECT: CRIMINAL JUSTICE DATA COMMUNICATIONS NETWORK (CJDN)

---

**1.0** PURPOSE:

The purpose of this policy is to provide for the physical security of Winona Police's Criminal Justice Data Network (CJDN) terminals 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. 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 Winona Police Department* is a Winona County Sheriff's Department staff member designated by the Sheriff. 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.

**2.0** POLICY

**2.1** Access to the CJDN shall be limited to employees who have been certified by the BCA to operate the terminal. The Chief of Police can designate Winona Police Department staff member(s) that have CJDN access. All other personnel of Winona Police Department must make their Criminal Justice inquiries through their CJDN operators.

**2.2** Staff having access to the CJDN system must meet the follow requirements

**2.2.1** Be an employee of Winona Police Department.

**2.2.2** Successfully pass a State and National fingerprint background check.

**2.2.3** Be trained and certified within six months of hire and biennially thereafter.

**2.3** New employees of the Winona 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.

**2.4** A potential new employee of the Winona 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.

WINONA POLICE DEPARTMENT

NUMBER: 102-11

PAGES: 4

EFFECTIVE DATE: February 15, 2012

---

SUBJECT: CRIMINAL JUSTICE DATA COMMUNICATIONS NETWORK (CJDN)

---

- 2.5 Fingerprint cards on CJDN operators will be kept in personnel files and cards of the IT personnel will be kept in their personnel files at Winona County.
  - 2.6 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 2 years. A list of these assigned passwords shall be kept in a locked location by a Winona County Sheriff's Department staff member designated by the Sheriff.
  - 2.7 Criminal history records can only be accessed for criminal justice purposes or other purposes authorized by law. CJDN inquiries for criminal history data must include the requesting officer's name, correct ORI, and the incident number associated with the request.
  - 2.8 Inquiries into the motor vehicle registration, driver license, criminal history or any other file in the MNJIS/NCIC systems will be performed for criminal justice purposes only.
  - 2.9 Terminals shall be secured from public access at all times.
  - 2.10 Printouts of data from the CJDN are to be disposed of by shredding or placing in the Shredd-It bins located throughout the department.
- 3.0 **Training of Sworn Officers:**
- 3.1 NCIC requires that all sworn personnel must receive basic, formal MNJIS/NCIC training within the first 12 months of hire, and annual refreshers thereafter. All training of sworn officers must be documented. A sworn officer includes any licensed peace officer, whether employed at the city, county, state or federal level.
  - 3.2 Winona Police Department will meet this requirement by having all officers watch the BCA's recorded training for MDT/MDC officers. The training is fifteen minutes long and will be viewed annually by sworn personnel. The Chief (or his/her designee) will provide the TAC with the required documentation for her/his records.

**4.0 Security of Terminal:**

- 4.1 The CJDN terminal(s) located within the Winona Police Department is/are in areas where there is no unescorted access.
- 4.2 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.
- 4.3 Criminal History responses, as well as all other CJDN printouts will be destroyed when no longer needed. These documents will be shredded at Winona Police Department.

**5.0 DEFINITIONS:**

- 5.1 CJDN is the overall system that provides access to data stored on state and national systems. It is comprised of many parts that allow for the exchange of data for criminal justice purposes.
- 5.2 Criminal Justice Information System (CJIS) – Minnesota specific information on wanted persons, missing persons, stolen property, etc. or what is commonly referred to as the “hot files”.
- 5.3 National Law Enforcement Telecommunications System (NLETS) – allows for interstate administrative messages to single or multiple agencies, DL checks: checks, boats snowmobiles, aircraft, etc. from other states.
- 5.4 National Crime Information Center (NCIC) – is a national collection center and index to existing state files, including III, which allows for interstate exchange of criminal history information.
- 5.5 CCH – Minnesota’s computerized criminal history information.

**6.0 APPROPRIATE USE/VIOLATIONS:**

- 6.1 Any employee misusing information or obtaining information for other

than official criminal justice purposes from the Criminal Justice Data Network will be subject to disciplinary action.

- 6.2** When performing any file inquiries or making any entries into NCIC or MNJIS, it is important to remember that the data stored in MNJIS/NCIC 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 NCIC and MNJIS is sensitive and should be treated accordingly, and unauthorized request or receipt of NCIC or MNJIS material could result in criminal proceedings.
- 6.3** When the Chief or the TAC becomes aware that an employee of Winona Police Department is using a CJDN terminal, CJDN terminal generated information, CJDN equipment, or CJDN access not in accordance with agency policies, state policies, or NCIC policies and said problem is not deemed merely operator error, the Chief or his designee, or the TAC shall promptly address the violation.
- 6.4** 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 Winona Police Department including verbal reprimand, written reprimand, suspension, or termination. Intentional misuse of the CJDN system 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.
- 6.5** The specific situation in each case of misuse of the CJIS system 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.
- 6.6** The Chief may at any time terminate a staff person's access to the CJDN system for any rule violation.