EAST RANGE POLICE DEPARTMENT

CJDN/MNIS

POLICY 110

REV 03/10/2025

I. MNJIS/CJDN

MNJIS/CJDN SECURITY POLICY

Section 1 shall be considered the official MNJIS/CJDN Security Policy for East Range Police Department. This section addresses the physical and personnel security of the MNJIS/CJDN system. 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 East Range Police Department shall be the person employed as the Administrative Assistant. The TAC manages the operation of the MNJIS/ 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 MNJIS/CJDN terminal.

ACCESS TO MNJIS/CJDN SYSTEM

Access to the MNJIS/CJDN shall be limited to employees who have completed BCA Certification. Currently, at East Range Police Department, this is limited to TAC and ATAC. All other personnel of East Range Police Department must make their Criminal Justice inquiries through their MNJIS/CJDN operators. The TAC shall be allowed to log into multiple sessions for the ability to perform administrative functions at different workstations and is not to be used for routine entries.

Staff having access to the MNJIS/CJDN system must meet the follow requirements:

(a) Be an employee of East Range Police Department.
(b) Successfully pass a State and National fingerprint background check.
(c) Be trained and certified within six months of hire and biennially thereafter.
(d) Complete Basic Security Awareness Training within six months of hire or assignment and annually thereafter. New employees of the East Range 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. A new employee of the East Range Police Department shall have a background check completed before they are hired. Fingerprint cards on MNJIS/CJDN operators are to be kept in a locked drawer by the Terminal Agency Coordinator. Fingerprint cards of the IT personnel that support the MNJIS/CJDN network will be at East Range Police Department. The TAC will issue a unique username and password to authorized users with access to the MNJIS/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 by the TAC in a locked cabinet.

TRAINING OF SWORN OFFICERS

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 employed at the East Range Police Department. DPD will meet this requirement by having all Officers review the BCA's recorded training for MDT/MDC Officers.

SECURITY OF TERMINAL

The MNJIS/CJDN terminal(s) and Criminal Justice Information for East Range Police Department is/are maintained in a secure area. Only authorized personnel who have passed a State and National fingerprint background check are allowed unescorted access to the secure area(s). 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 MNJIS/CJDN printouts will be destroyed when no longer needed. These documents will be shredded at East Range Police Department. All personnel who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS systems must also take Security Access training and pass the test.

II. MISUSE OF MNJIS/CJDN SYSTEM

MNJIS CJDN –is the overall system, which provides criminal justice agencies computer access to data stored on state and national systems. 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. 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.

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.

When the Chief or the TAC becomes aware that an employee of East Range Police Department is using a MNJIS/CJDN terminal, MNJIS CJDN terminal generated information, MNJIS CJDN equipment, or MNJIS 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 their designee, or the TAC shall promptly address the violation. The Chief or their 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 East Range Police Department. Intentional misuse of the MNJIS/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. The TAC, with the Chief's approval, may at any time terminate a staff person's access to the MNJIS/CJDN system for any rule violation.

III. HIT CONFIRMATION

DEFINITION OF A CJIS/NCIC HIT

A Hit is a positive response from MNJIS and/or NCIC in which the person or property inquired about appears to match the person or property contained in the response. Queried subject appears to match the record subject.

NCIC HIT CONFIRMATION POLICY

Agencies that enter records into MNJIS/NCIC must be available for Hit confirmation 24 hours a day, every day of the year. Non-24-hour agencies must place either the ORI or the telephone number (including area code) of the 24-hour agency responsible for responding to a hit confirmation request in the MIS field of the hot file record.

THE HIT CONFIRMATION PROCESS

NCIC policy requires an agency receiving a hit on another agency's MNJIS/NCIC record to contact the entering agency to confirm that the record is accurate and up to date.

The agency requesting confirmation must specify whether the request is ROUTINE or URGENT. ROUTINE hits allow up to an hour to respond and URGENT hits allow only ten(10) minutes. See current NCIC manual for entry procedure. Routine hit confirmation requests must be responded to within one(1) hour. Urgent hit confirmation requests must be responded to within ten (10) minutes.

HIT CONFIRMATION POLICY

If you have performed an inquiry and received a "Hit", use the following procedures:

(a) Print a hard copy of the Hit.
(b) Immediately confirm with the arresting officer. Examine the Hit message and evaluate all information in the record and compare with the officer's description of the subject being stopped or property being recovered to insure that person or property matches the person or property described in the Hit.
(c) Confirm the Hit with the originating agency. An inquiring agency that receives a hit must use the YQ message to request confirmation of a Hit. Use the appropriate preformatted screen.

HIT CONFIRMATION RESPONSE

If you receive a Hit confirmation, use the following procedures to respond.

(a) Print a hard copy of the confirmation request.
(b) Note the amount of time that you have to respond and make sure to respond within that time period.
(c) Attempt to confirm the Hit by checking the original warrant or report file to determine if the person is still wanted or property is still missing.

(d) If you are unable to confirm the Hit, send a response with an explanation for not being able to confirm.

DOCUMENTATION OF THE HIT CONFIRMATION PROCESS

All Hit confirmation teletypes should be retained, and precise notes should be made on the printout concerning how, when, and to whom the information was given. The printout should be kept in the case file. Documentation of the confirmed Hit is essential and may be critical to the success of defending a later claim of misidentification or false arrest.

IV. MISSING PERSON POLICY

ENDANGERED MISSING PERSONS

Endangered missing persons, regardless of age, are to be entered into the system immediately not to exceed two (2) hours, upon receiving the minimum data required for entry into NCIC. The two (2) hour clock shall begin at the time the minimum data required is received. The agency must be able to document the time.

JUVENILES - UP TO 17 YOA

Juveniles are to be entered into the system immediately, not to exceed two hours, upon receiving the minimum data required for entry into NCIC. The two hour clock shall begin at the time the minimum data required is received. The agency must be able to document the time.

ADULTS 18-20 YEARS OLD

Any adults under 21 years of age are to be entered into the system immediately, not to exceed two (2) hours, upon receiving the minimum data required for entry into NCIC. The two (2) hour clock shall begin when the minimum data required for entry is received from the complainant. The agency must be able to document the time. A signed report is not required.

ADULTS 21 YEARS AND OLDER

To ensure maximum System effectiveness, Missing Person records must be entered immediately when the conditions for entry are met, not to exceed three(3) days, upon receipt by the entering agency. Adults, age 21 and older, are required to have signed documentation supporting the stated conditions under which they are being declared missing before entry into the system, unless they are victims of a catastrophe.

Entry of All Missing People

The documentation should be from a source such as a parent, legal guardian, next of kin, physician or other authority source including a neighbor or a friend. However when such documentation is not reasonably attainable, a signed report by the investigating officer will suffice. For agencies using Electronic Records Management Systems (ERMS), some forms of signatures that are acceptable are:1) Digitized signatures 2) Manual signatures scanned into the ERMS 3) The case officer's typed name into the

report in the ERMS. When entering records into the NCIC missing person file, the entry person will:

(a) Run a current DVS and CCH/III inquiry to obtain as many descriptors as possible regarding the subject. This check should include a check of whether medical/dental information is available regarding the subject.
(b) Any descriptors used must be documented in the officer's report or saved within the case file.
(c) Attempts to obtain medical/dental information must also be documented in the case file.
(d) Enter a record into NCIC on the subject. This record should include all descriptors. Additional identifiers such as scars, marks and tattoos, aliases, additional dates of birth, etc., should be added to the record through the use of the Enter Missing Person Supplemental Screen.
(e) After the record is entered, query the NCIC entry to obtain a hard copy for second party verification purposes.

Agencies are required to verify and update NCIC 2000 missing person record entries with any additional information, including: Blood Type (BLT); Dental Characteristics (DCH); Fingerprint Classification (FPC); Jewelry Type (JWT); and Scars, Marks, Tattoos, and Other Characteristics (SMT) within sixty (60) days of entry. If a record has a date of entry older than thirty (30) days and any of the above fields are blank, a $.K. Missing Information Notification identifying the blank fields will be transmitted. The $.K. Missing Information Notification will also include the record.

A notation shall be made in the case file indicating when this attempt was made and what the outcome was, i.e.: child has returned, dental records obtained, etc. This sixty (60) day update is a mandatory FBI requirement on all missing persons records under the age of 21 and East Range Police Department personnel shall document this attempt in the case file to show that this requirement has been met.

V. SECOND PARTY CHECKS

Second party checking means that someone, other than the person making the record entry, checks the record for accuracy and completeness. This procedure is required for ALL Hot File entries and modifications to record entries. The person conducting a second party check on a hot file should first query the record, print the HIT, and proceed with the following steps:

Ensure that all appropriate sources were checked and queried for complete information. This may include Criminal History records, motor vehicle registrations, driver's license information and any other available sources. Make sure that this source material is kept with the case file or warrant.ie: D/L printouts, Registration printouts, CCH/III identification information

Compare the information from the sources listed above against the record entered into MNJIS/ NCIC to verify the accuracy of information in all fields of the hot file record. Verify that all information was coded correctly with appropriate up-to-date NCIC codes. Correct any records that are inaccurate or coded incorrectly. Verify that the record was "packed"

with all available information. Initial the hard copy of the entry and place the hard copy in the case file.

VI. IDENTITY THEFT

Before an entry can be made in the Identity Theft File, an official complaint (electronic or hard copy) must be recorded and on file at our law enforcement agency. Our agency may make an NCIC Identity Theft entry only if we are the agency that takes the identity theft complaint and the following criteria are met:

1. Someone is using a means of identification of the victim.

2. The identity of the victim is being used without the permission of the victim.

3. The victim's identity is being used, or intended to be used, to commit an unlawful activity.

4. The victim must sign a consent waiver, which can be found on the CJDN Secure site, prior to the information being entered into the Identity Theft file.

5.Information on deceased persons may be entered into the file if it is deemed by the police Officer that the victim's information has been stolen. No consent form is required with the entry of deceased person information.

6.If the Identity Theft file is going to contain the Social Security Number of the victim, our agency is required to inform the individual of this fact and they must sign the "Notice about Providing Your Social Security Number" form, which can be found on the CJDN Secure site.

VII. PROPERTY HOT FILE RECORDS

VEHICLE FILE

Before entering a stolen or felony vehicle record into MNJIS/NCIC you should:

1. A theft report describing the stolen item including the serial number (SER) or owner applied number (OAN).

2. Do a registration check with the state that the vehicle is registered with and print out a hard copy of the registration to attach to the record.

3. Enter the record into MNJIS/NCIC using the pre-formatted screen. Make sure to pack the record with as much information about the vehicle as is available. Also verify the NCIC codes as they are not always the same as what you see on the copy of the registration.

4. Query MNJIS/NCIC to verify entry and to obtain a copy of the record to be attached to the record.

5. Follow procedures for the second party check.

STOLEN GUNS, ARTICLES, BOATS AND SECURITIES

Before entering a stolen record into MNJIS/NCIC you should:

1. A theft report describing the stolen item including the serial number (SER) or owner Applied number (OAN).

2. If entering a boat, do a registration check with the state that the boat is registered with and print out a hard copy of the registration to attach to the record.

3. Enter the record in MNJIS/NCIC using the pre-formatted screen. (Boats and securities will only be entered into NCIC.) Make sure to pack the record with as much information about the item as is available.

4. Query MNJIS/NCIC to verify entry and to obtain a copy of the record to be attached to the record.

5. Follow procedures for the second party check.

VIII. VALIDATION

Validation obliges the ORI to confirm that the record is complete, accurate, and still outstanding or active.

The East Range Police Department must validate all hot file records, except for Article File records. Validation takes place 60-90 days from the date of entry and yearly thereafter.

Validation requires the entering agency to remove all records that are no longer active from the MNJIS/NCIC Hot Files.

Validation requires the entering agency to compare all records against the current supporting documentation to ensure that the information in each field is accurate; and that the records contain all available information found in the case files.

Validation requires the entering agency to remove all records for which corresponding case file documentation cannot be located OR recreate the case file so our agency meets NCIC requirements.

Validation requires the entering agency to update records as needed when NCIC Code changes occur; Agency related information, such as extradition limits or hit confirmation, and/or contact information changes; or new or additional information becomes available.

The following are contacts: (1) Missing Person - consult the complainant to verify that the person is still missing for all missing person records.

(2) 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.

Note: All entries in any of the Hot Files must be documented for entry. In addition, upon the entry of any Hot File, a second party check must be completed.

IX. DISPOSAL

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by MN BCA and FBI security policies.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

A. Shredded using East Range Police Department issued cross-cut shredders
B. Placed in locked and secured container as to be destroyed by Shred It Corp.
C. Incineration using incinerators or witnessed by ERPD personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) Shall be disposed of by one of the East Range Police Department employees

A. **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
B. **Degaussing -** a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
C. **Destruction –** a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from East Range Police Department control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

X. REFERENCES AND REVISIONS

I. References

a. Duluth Police Department policy 808
b. FBI NCIC Security Policy B.
c. BCA MNJIS TAC Responsibilities Handbook

II. Revisions

a. 04/19/2016 – Initial Policy
b. 03/10/2025 – ERPSB approval Date.

EAST RANGE POLICE DEPARTMENT

COMPUTER SECURITY INCIDENT RESPONSE PLAN

SEPTEMBER 2023

PURPOSE

This document describes the East Range Police Departments plan for responding to both physical and electronic information security incidents. This plan shall apply to the physical location(s), the information systems, all Criminal Justice Information (CJI), data, networks and any person or device of the East Range Police Department that gains access to these systems or data.

Indicators of incidents are including but not limited to:

- Malware/Viruses/Trojans
- Ransomware
- Phishing
- Unauthorized electronic access
- Breach of Information
- Unusual, unexplained, or repeated loss of connectivity
- Unauthorized physical access
- Loss or destruction of physical files, etc.
- Any other suspicious activity on device

PREPARATION

The East Range Police Department has policies and procedures in place and utilizes several mechanisms to prevent and respond to an incident including but not limited to:

- Security Awareness Training for all personnel. This training must be updated every two years.
- Malware/Antivirus/Spyware Protections. All information system terminals are protected with updated and continuous protection without the need for the station holders' intervention. Each station holder is restricted from accessing, modifying, disabling or making other changes to the defense mechanisms.
- Firewalls within the network to provide the necessary depth of defense
- Personal security measures
    - All East Range Police Department personnel with access to CJI or those areas where CJI is accessed, stored, modified, transmitted, or maintained have been cleared and trained to standards to have access to those areas.

INCIDENT REPORTING AND POST INCIDENT ACTIVITY

In the event that an incident has occurred or is suspected to have occurred involving CJI, the Chief Information Security Officer (ISO), TAC or Local Agency Security Officer (LASO) shall be notified immediately.

Information to be reported immediately:

- What happened? What time(s)?
- What terminal or network was being used?
- Incident Reporter
- What, if any actions were taken

The incident investigator shall review the suspected incident, complete a security incident response report (form MNJIS-F-5012) and email the report to the Minnesota BCA ISO within 24 hours of initial discovery.

Post incident activities will occur after the detection, analysis, containment, eradication and recovery form a security incident

REFERENCES AND REVISIONS

REFERENCES

1. ERPD SAFETY PLAN

REVISIONS

1. 09/2023 – INITIAL PLAN

EAST RANGE POLICE DEPARTMENT

110.a COMPUTER SECURITY INCIDENT RESPONSE PLAN

SEPTEMBER 2023

PURPOSE

This document describes the East Range Police Departments plan for responding to both physical and electronic information security incidents. This plan shall apply to the physical location(s), the information systems, all Criminal Justice Information (CJI), data, networks and any person or device of the East Range Police Department that gains access to these systems or data.

Indicators of incidents are including but not limited to:

- Malware/Viruses/Trojans
- Ransomware
- Phishing
- Unauthorized electronic access
- Breach of Information
- Unusual, unexplained, or repeated loss of connectivity
- Unauthorized physical access
- Loss or destruction of physical files, etc.
- Any other suspicious activity on device

PREPARATION

The East Range Police Department has policies and procedures in place and utilizes several mechanisms to prevent and respond to an incident including but not limited to:

- Security Awareness Training for all personnel. This training must be updated every two years.
- Malware/Antivirus/Spyware Protections. All information system terminals are protected with updated and continuous protection without the need for the station holders' intervention. Each station holder is restricted from accessing, modifying, disabling or making other changes to the defense mechanisms.
- Firewalls within the network to provide the necessary depth of defense
- Personal security measures
    - All East Range Police Department personnel with access to CJI or those areas where CJI is accessed, stored, modified, transmitted, or maintained have been cleared and trained to standards to have access to those areas.

INCIDENT REPORTING AND POST INCIDENT ACTIVITY

In the event that an incident has occurred or is suspected to have occurred involving CJI, the Chief Information Security Officer (ISO), TAC or Local Agency Security Officer (LASO) shall be notified immediately.

Information to be reported immediately:

- What happened? What time(s)?
- What terminal or network was being used?
- Incident Reporter
- What, if any actions were taken

The incident investigator shall review the suspected incident, complete a security incident response report (form MNJIS-F-5012) and email the report to the Minnesota BCA ISO within 24 hours of initial discovery.

Post incident activities will occur after the detection, analysis, containment, eradication and recovery form a security incident

REFERENCES AND REVISIONS

REFERENCES

1. ERPD SAFETY PLAN

REVISIONS

1. 09/2023 – INITIAL PLAN