

# Keweenaw Bay Indian Community

## Policy and Procedures Use and Security CJIN and LEIN Networks

### **Purpose:**

To establish a policy and procedures for the use and security of Criminal Justice Information (CJI) obtained through the Criminal Justice Information Network (CJIN) including but not limited to access to the National Crime Information Center (NCIC) International Justice and Public Safety Network (NLETS) Interstate Identification Index (III) and Michigan's Secretary of State (SOS) databases, and maintenance and security of all access terminals and equipment used to obtain CJI. CJIN terminals are computer workstations and related equipment used to access CJI through either the Justice Telecommunications System (JUST) or the State of Michigan Law Enforcement Information Network (LEIN).

### **Policy:**

It shall be the policy of the Keweenaw Bay Indian Community that all employees having access to the CJIN shall comply fully with all tribal and federal laws and regulations applicable to CJIN and with these policies and procedures.

### **Procedures:**

CJIN: CJI via JUST or LEIN Systems - NCIC/NLETS/III/SOS databases.

- A. Only authorized department personnel, who have been fingerprinted, and background checked will have access to CJI. Only authorized department personnel, who have been fingerprinted, background checked and trained shall operate the CJIN terminals. All employees who will have access to the CJIN terminals must submit to a background investigation and be approved by the Local Agency Security Officer (LASO) for access. All authorized personnel will be background checked with at least a name based records check at least once every five years. All terminal users must sign the LEIN Use Agreement prior to gaining access to the terminals.
  - 1. CJIN terminals (JUST and LEIN) are located in and operated by the Keweenaw Bay Tribal Police Department. Requests for CJI by an agency with access to CJI shall be run by qualified users of the system using the ORI of the agency making the request.

2. CJIN terminals shall be kept in a locked and secure area. Network equipment shall be kept in a secure and locked equipment rack. Access to secure areas is limited to authorized personnel. All support staff including contractors and custodial staff who have authorized access to secure areas must be fingerprinted and background checked according to the standards describes in Procedures, part A. Contractors, custodians and other unauthorized personnel must be escorted in secure areas at all times during CJI processing.
  3. An activity log shall be kept with each CJIN terminal and any time the terminal is used it shall be recorded in the log including date of transaction, identity of the person/vehicle/title/or item run through the JUST or LEIN system, reason for the look-up, the name of the authorized user using the terminal, and the name of the person/agency requiring the information.
  4. Requests for access to the CJIN terminal and network equipment for maintenance and security purposes shall be submitted to the LASO for approval prior to access. Once approved this access to the terminal shall also be recorded in the log.
  5. Once every six months the LASO shall provide the head of each department having authorized CJI access a list of names authorized to access CJI for that department. The department head shall respond within three working days and confirm those persons who should be authorized for access to CJI and submit Notice of Termination of CJI Access forms for each employee who should not have LEIN access but is on the LASO's list.
- B. A CJIN Terminal Agency Coordinator (TAC) will be appointed for each department requiring access to CJI. TACs will re-certify all operators of CJIN terminals every two years. Re-certification will include a test on the JUST and/or LEIN system, review of the Security Awareness power point, a criminal history and driving record check.
- C. CJIN terminal operators shall only use CJIN terminals for those purposes which they are authorized.
- D. It is a violation of this policy, as well as tribal, state and federal law, to release any information to unauthorized persons, such as driver's license information or criminal history checks.
- E. Reports requiring NCIC entry shall be entered in a timely manner, which is hereafter defined as 72 hours. These are to include runaways, missing persons, stolen autos, missing or stolen articles, warrants, personal protection orders, etc.

- F. Once a warrant has been authorized, records personnel are to ensure that NCIC entry has been completed within the seventy—two (72) hour time period, per NCIC policy. Warrants will not be held without entry into NCIC.
- G. When confirming out-of-state hits, the hit confirmation response or request screens shall be used.
- H. Users are required to maintain the confidentiality of CJI by taking adequate measures to ensure that unauthorized person(s) do not view information printouts or screens. When leaving your work station, you MUST log out of the JUST or LEIN system.
- I. No unauthorized LEIN messages are to be sent for general broadcast or to any other agency. Messages may be sent to a maximum of six areas. Statewide broadcasts must be sent through the Michigan State Police East Lansing Operations (ELOP).
- J. Monthly Warrant Validations are to be accomplished by authorized TAC personnel in a timely manner.
- K. At no time shall Criminal History Record Information (CHRI) printouts be released to unauthorized persons or entities. LEIN is not governed by FOIA. All CJIN or LEIN information shall be redacted from police reports.
- L. Secondary dissemination is allowed to the prosecutor and courts. Dissemination shall be documented on the coversheet of the report in the following manner: CCH to TAO (for Tribal Attorney's Office) or Courts/by (insert officer's last name).
- M. Missing persons age 21 and older shall be entered into LEIN/NCIC upon receipt of the information and proper documentation using Michigan's Missing Persons Report form. You must have a signed authorization prior to entry to protect privacy.
- N. Missing persons under the age of 21 must be entered into LEIN/NCIC within two hours of obtaining proper information for entry. You do not need a signature for entry of missing persons under the age of 21.
- O. LEIN, NLETS or other related CJIN messages, such as stolen vehicles, missing or wanted subjects, or officer safety issues, shall be placed on the Tribal Police Bulletin Board for officers to read. Once they have been recalled or purged, they shall be placed in a certified document destruction bin.
- P. The procedure for entry of second party checks, validation, cancellation or recalling of all NCIC or LEIN entries shall be completed per the corresponding NCIC or LEIN Manual.

- Q. LEIN, NCIC and all other confidential manuals shall be maintained in a secured area of the Police Department and the Motor Vehicle Division.
- R. Fire departments that have a signed memorandum of agreement with this department may request and receive LEIN information, in the form of a printout or otherwise, through this agency for the following purposes:
  - 1. A pre-employment criminal conviction history (purpose code "E" only) check.
  - 2. A pre-employment driving record check.
  - 3. Vehicle registration information for vehicles involved in a fire or hazardous material incident.

#### CJIN WORKSTATION PASSWORD GUIDELINES:

- A. JUST or LEIN password must be changed at least every 90 days.
- B. These passwords must be at least eight characters with at least two letters and two numbers.
- C. A strong password would contain both upper and lower case characters and have digits and punctuation characters as well as letters i.e.:  
!@#\$%^&\*()\_+{ }:";<>?,.
- D. User accounts with access to JUST or LEIN privileges will have a unique password from all other accounts held by that user.
- E. Users shall not use their user id as their password.
- F. Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- G. All user logins that are no longer needed will be disabled. i.e.: When a user retires, quits, etc. Departments with access to CJIN terminals shall submit Notice of Termination of JUST or LEIN Access forms to the LASO as soon as they are aware that an employee will not be available or allowed to access JUST or LEIN.

#### UNIQUE IDENTIFIERS

- A. A unique identifier shall be created for all CJIN terminal users in order to ensure accountability of all users who access Keweenaw Bay Indian Community's network and network devices.

- B. The Keweenaw Bay Indian Community requires users to identify themselves uniquely before the user is allowed to perform any action on the network and/or applications.
- C. All user IDs shall belong to currently authorized users. Employees shall not share their IDs with other employees, supervisors, management, or family at any time.

## DISPOSAL OF MEDIA

- A. When no longer usable, diskettes, tape cartridges, ribbons, hard and other digital media storage or other similar items used to process or store classified and/or sensitive data shall be properly disposed of by the LASO.
- B. All printouts stored by agencies with CJI access shall be properly stored. When no longer usable, printouts of CJI data shall be placed in properly marked document destruction bins.
- C. IT systems that have processed, stored, or transmitted sensitive and/or classified information shall not be released from the Keweenaw Bay Indian Community's control until the equipment is sanitized and all stored information has been cleared. For sensitive, but unclassified information, the sanitation method shall be approved by the Keweenaw Bay Tribal Police Department. For classified systems, National Security Association approved measures shall be used. The following procedures will be followed:
  - a. Employees will send all hardware that processes and/or stores classified and/or sensitive data to the Keweenaw Bay Indian Community's Information Technology Personnel to be properly disposed. The hard drives must be wiped to DOD level three specifications (7 wipes) and destroyed properly.
  - b. The Keweenaw Bay Indian Community's Information Technology Personnel will dispose of hardware by Overwriting, Demagnetizing or Destruction.
  - c. Computers that are used to transmit classified and/or sensitive information must protect residual data. This will be accomplished with the use of integrated encryption technology. This technology uses a device or software which encrypts all data as it is written to disk. When the user retrieves a file, the data is automatically decrypted for the owner to use. This encryption/decryption process is typically transparent to the user. Should the hard drive be removed, no useable data can be retrieved.

## LEIN USE AGREEMENT

Every employee with authorized access to CJIN Systems/CJI must sign the LEIN Use Agreement wherein the employee submits to the criminal jurisdiction of the Keweenaw Bay Indian Community for purposes of prosecution for misuses of his or her access to JUST and/or LEIN.

### **Violations of these Policies and Procedures:**

Any violation by a terminal user of these policies and procedures could result in denial of access to JUST or LEIN. Accordingly, the following progressive sanction process will be used to enforce these policies and procedures while cooperating with agencies to continue to protect the integrity of the system and its users.

Step 1: Notice of the alleged violation from the JUST Criminal Justice Information Systems Officer (CSO) or LIEN Field Services will be sent to the Department Head for the agency where the alleged violation is to have occurred. The agency whose employee committed the violation must send a response to the JUST CSO or LEIN Field Services within 45 days of the incident with the proposed resolution or status of the investigation and any violation must be corrected with documentation to the JUST CSO or LEIN Field Service's satisfaction within 90 days from the date the notice is sent or Step 2 will be initiated. Unsatisfactory progress in Step 1 will result in the initiation of Step 2.

Step 2: Notice of delinquency is sent to the Department Head and the CEO of the Keweenaw Bay Indian Community. Any requests for additional LEIN access will be held in abeyance. If compliance is not documented within 30 days, Step 3 will be initiated.

Step 3: Access to JUST or LEIN will be limited. Computerized Criminal History (CCH) inquiries and Administrative Messages will be denied. Notice of delinquency and the denial is sent to the Department Head, the President of the Keweenaw Bay Indian Community, the Tribal Prosecutor, and the Chief Judge of the Keweenaw Bay Indian Community Trial Court and to each serviced agency. If compliance is not documented within 30 days, the matter will be referred to the Criminal Justice Information Systems Officer (CSO) for the initiation of Step 4.

Step 4: The agency shall no longer be permitted to participate in JUST or LEIN. All terminal equipment will be removed. The agency shall remain responsible for any unpaid fees due to JUST or LEIN up to this date.

Direct access to JUST or LEIN shall only be reinstated after review and approval by the CSO. The agency may institute an indirect access user agreement with another agency, but this shall be limited to inquiry capabilities only and excludes access to the criminal history record information and NCIC III files.

Note: Extensions to respond to the progressive sanction process may be authorized by the CSO if circumstances warrant such action.

**Violations of Tribal Code:**

Any employee who misuses the employee's access to LEIN and or NCIC, in violation of §3.611 of the Tribal Code, will be referred for prosecution in Tribal Court and may also be subject to applicable federal or state penalties.