CHAPTER # 26 POLICE INFORMATION	POLICY # 26.5 CJIS SECURITY
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.	
Date Implemented: 11/01/2019	Review Date:

POLICY

The Indian Hills Police Department utilizes LINK/NCIC in the performance of daily operations. The ability to access records, make inquiries, and communicate with the criminal justice community is vital in providing a safe and secure environment.

DEFINITIONS

CJI – Criminal Justice Information

CJIS – Criminal Justice Information Services

LINK – Law Enforcement Information Network of Kentucky

NCIC – National Crime Information Center

NLETS – National Law Enforcement Telecommunications System

CTA – Control Terminal Agency

OAN – Owner Applied Number

Hit – A message indicating that a person or item is entered in the LINK and/or NCIC system

PROCEDURE

The LINK, NCIC, and NLETS system(s) shall not be used to send regional broadcast messages for the following:

- Social Announcements (i.e. holiday messages or retirements)
- Personnel Recruitment
- Messages in which the complainant is interested only in the recovery of property
- Attempt to locate vehicle when no prosecutions will be pursued
- Excessively long messages
- Support or opposition of political, legislative bills, or labor issues
- Announcements of political, legislative bills, or labor-oriented meetings
- Requests for information on salary, uniforms, personnel, or related topics

- Advertisement or sale of equipment
- No messages regarding wanted subjects or vehicles if they can be entered into NCIC
- Requests for criminal history record information
- No reply only if wanted
- Solicitation of funds
- Training announcements identifying the name of “for profit” companies providing training

The LINK, NCIC, and NLETS system(s) shall be used for official business only and shall not be used for personal business or interests.

User Agreements

The Department will maintain on file the appropriate and current user agreement:

- Between this agency and the Kentucky State Police
- Between this agency and the Jefferson County Sheriff’s Office
- Between this agency and Louisville-Jefferson County MetroSafe
- Between this agency and each respective non-criminal justice agency

Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI, to include all personnel who have unescorted access to a physically secure location. This applies to agency employees as well as to vendors and contractors who access the location or system.

Auditing and accountability

Currently the state information system shall generate audit records for defined events indicating what events occurred, the source of the event, and the outcome of the event. The state system periodically reviews and updates the list of agency-defined auditable events and has an operation information security incident response policy which includes written report procedures. The Department will report any perceived events to KSP.

Incident response

The Department will report any security incident involving CJI to KSP as soon as practical.

Identification and authentication

The Department will follow CJIS Security Policy for password authentication. Each password will:

- Be a minimum in length of eight (8) characters on all systems
- Not be a dictionary word or proper name
- Not be the same as the User ID
- Expire within a maximum of 90 calendar days
- Not be identical to the previous ten (10) passwords
- Not be transmitted in the clear outside the secure location
- Not be displayed when entered

The Department will use advanced authentication for personnel who access and/or manage information systems containing CJI from non-secure locations (Examples include tokens, smartcards, etc.).

Media protection

To ensure that access to digital and physical media in all forms is restricted to authorized individuals, the Department shall:

- Securely store all media within physically secure locations and controlled areas.
- Restrict access to all media to authorized individuals.

- Protect and control all media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
- Degauss or overwrite digital media prior to disposal or release for reuse by authorized individuals. Inoperable media shall be destroyed.
- Ensure the sanitization and/or destruction is witnessed or carried out by authorized personnel and maintain written documentation of the steps taken to sanitize or destroy electronic media.
- Ensure all physical media is destroyed by shredding or incineration, and ensure the disposal is witnessed or carried out by authorized personnel.

Physical protection

The Department shall document and implement all physical protection policy requirements according to the CJIS Security Policy, to include:

- The perimeter of the secure location shall be prominently posted and separated from non-secure locations by physical controls.
- Issue credentials to authorized personnel or maintain a current list of personnel with authorized access to the secure location.
- Control physical access points and verify individual access before granting access.
- Control physical access to information system distribution and transmission lines within the physically secure location.
- Control physical access to CJI on any computer by:
    - Positioning information system devices that display and print CJIS information in such a was as to prevent unauthorized individuals from accessing and viewing CJI.
    - Ensuring information on the LINK/NCIC computer is not viewed by unauthorized persons.
    - Ensuring only actively manned consoles have the screen operational. All unmanned consoles should have the CJIS screen turned off or locked.
- Monitor physical access to the information system to detect and respond to physical security incidents.
- Escort visitors at all times and monitor visitor activity.
- Authorize and control information system-related items entering and exiting the physically secure location.
- All information transmitted through LINK, NCIC, and/or NLETS shall be considered confidential and shall be disseminated only for official purposes.

<u>Mobile devices</u>

The Department shall authorize, monitor, and control Mobile Data Terminals and other wireless access to information systems containing CJI.

<u>Requesting LINK/NCIC entry</u>

An Officer shall consider requesting LINK/NCIC entry when taking reports of stolen items, wanted persons, and/or missing persons.

Firearms, computer equipment, vehicles, and items over $300 shall be entered into LINK/NCIC if the item has a known unique identifier.

The Officer requesting LINK/NCIC entry shall complete the appropriate entry form located in the squad room.

The Officer shall provide the entry form and a copy of the offense report to the communications center. This can be submitted via e-mail, fax, or hand delivered.

<u>Hazardous materials inquiry</u>

At the request of an Officer, the communications center shall inquire NLETS form information on hazardous materials.

The Officer will provide the four-digit (placard) code to the communications center. Information from NLETS should include the chemical name, personal safety precautions, general handling procedures, disposal methods, degree of hazard to the public, and availability of counter-measure materials.

Misuse

Reports of violation of departmental, state, or federal policies and regulations regarding CJIS, CJI, NCIC, NLETS and/or LINK, misuse of CJIS equipment or information will be reported to The Chief of Police.

Reports of violation of departmental, state, or federal policies and regulations regarding CJIS, CJI, NCIC, NLETS and/or LINK, misuse of CJIS equipment or information will be reported to the department's assigned CJIS auditor. The auditor will be updated as to the findings of the investigation and any disciplinary actions taken.

Reports of violation of departmental, state, or federal policies and regulations regarding CJIS, CJI, NCIC, NLETS and/or LINK, misuse of CJIS equipment or information will be investigated in accordance with the Department's Policies and Procedures.

Persons found to be in violation of departmental, state, or federal policies and regulations in regard to CJIS, CJI, NCIC, NLETS and/or LINK, issue of CJIS equipment or information, will be subject to disciplinary action in accordance with applicable policies of the Department, up to and including termination.