Pippa Passes Police Department
100 Purpose Road
Pippa Passes, KY 41844

CJIS, LINK, NCIC, and NLETS

Subject: CJIS, LINK, NCIC, and NLETS

Purpose: The purpose of this guideline is to establish policies for the use and security awareness for CJIS, LINK, NCIC, and NLETS, and to define the departments officers and roles.

Scope: This procedure applies to all members of the Pippa Passes Police Department

General: The Pippa Passes Police Department utilizes LINK, NCIC, NLETS, and all CJIS programs to perform daily operations. Accessing records, making inquiries, and communicating with the criminal justice community are vital in providing a safe and secure environment.

PROCEDURE:

General Use and Restrictions

1. CJIS users and all PPPD personnel shall adhere to federal and state laws, regulations, procedures, and policies adopted by the NCIC Advisory Policy Board, FBI/NCIC, NLETS, LINK, and CSA relating to system operation and the security and privacy of criminal justice and law enforcement information.
2. The Pippa Passes Police Department adheres to the LINK/NCIC policy and CJIS Security Policy. Policies can be viewed at www.alc.edu/student-life/campus-safety/
3. Each user shall monitor the LINK/NCIC accessed computer continuously while they are logged on to the computer and have an active CJIS session open
4. The LINK, NCIC, NLETS, and any CJIS system(s) shall be used for official business only and not for personal business or interests.

Roles and Responsibilities

Terminal Agency Coordinator (TAC)- Phillip Slone

1. Terminal Agency Coordinator (TAC) will serve as the point of contact at the local agency for matter relating to CJIS information access.
2. The TAC administers CJIS system programs with the local agency and oversees the agency's compliance with CJIS systems policies.
3. The TAC will carry out all TAC duties as outlined in the LINK Policy.
4. The TAC will complete any mandated TAC training.

Assistant Terminal Agency Coordinator (ATAC)

1. The ATAC will assist in the TAC duties and will act as the TAC in the event the TAC is unable to perform duties.
2. The ATAC will complete any mandated TAC training.

Local Agency Security Officer (LASO)- Phillip Slone

1. Identify who is using the CJIS, LINK, NCIC, NLETS platforms and ensure no unauthorized individuals have access.
2. Identify and document how the equipment is connected to the state system.
    a. This will be shown with a network map diagram
3. Ensure that personnel security screening procedures are being followed.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.
6. LASO will complete Security Role level of Security and Privacy Training in CJIS OnLine and any other mandated training as required.
7. The Pippa Passes Police Department insures the designated employee will complete the LASO training yearly.

User Agreements

1. This agency will maintain on file the appropriate and current user agreement:

    a. Between this agency and the Kentucky State Police, and each respective satellite agencies
    b. If secondary dissemination is allowed, a secondary dissemination log must be kept

2. This agency will implement and maintain on file the CJIS Security Addendum with each servicing private contractor and vendor.

CJI Access

All personnel that the department will request access to CJI will submit fingerprints at an IdentoGo location before requesting access to CJI.

This agency will ensure the correct User Account Request form is sent to the ISO when fingerprint submission has been completed.

Terminal Operator's, Inquiry Only and MDT User's

This agency will ensure the CJIS user takes the respective training Full Access, or MDT/Inquiry Only immediately in the NexTest program on the CJIS LaunchPad.

Security and Privacy Training and Roles

1. Security and privacy training shall be required before CJIS access and yearly thereafter for all personnel with access to Criminal Justice Information (CJI), including PPPD employees only requiring physical and logical access and will not be using the CJIS 10-8 system. The PPPD will keep documentation on file consisting of those names that should have CJIS 10-8 access with a copy of their certificate, as well as those that have been submitted for access but has not had training yet. Files with certificates will also be kept for those employees who require CJIS level 2 clearance.

    a. **Security and Privacy: Basic Role- Personnel with Unescorted Access to a Physically Secure Location**
    (This level is designed for people with access to a secure area but are not authorized to use CJI. They are required to complete the level two security awareness training)
    b. **Security and Privacy: General Role- All Personnel with Access to CJI**
    (This level is designed for authorized people to access an information system that provides access to CJI. They are required to take the Inquiry Only training.)
    c. **Security and Privacy: Privileged Role- Personnel authorized to perform security-relevant functions**
    (This level is designed for all information technology personnel, including system administrators, security administrators, network administrators, etc.... This role shall have taken general Data Awareness Classes)
    e. **Security and Privacy: Security Role- Organizational Personnel with Security Responsibilities (LASO)**
    (This level is designed for personnel responsible for ensuring the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJIS Security Policy. This role shall have taken the Inquiry-only training as well as the LASO training.)

    ❖ All Pippa Passes Police Department personnel will be required to take a Data Awareness Class from a 3rd party vendor. Certificates will be provided.

Auditing and Accountability

1. 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. This agency will report any perceived events to KSP.

2. For CAD Systems, Record Management Systems (RMS), Web based CPI Open Fox, Etc. the agency 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 agency will periodically review and update the list of agency-defined auditable events and has an operation information security incident response policy, which includes written report procedures. This agency will report any perceived events to KSP.

Incident Response

1. The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.
2. This agency shall have its own Security Incident Response Policy with reporting procedures in place.
3. This agency will report all incidents to KSP

Identification and Authentication

1. This agency will follow CJIS Security Policy for password authentication. Each password will:

    a. Be a minimum in length of eight (8) characters on all system.
    b. Not be a dictionary word or proper name.
    c. Not be the same as the Userid. The Userid cannot be included in the password.
    d. Expire within a maximum of 120 calendar days.
    e. Not be identical to the previous ten (10) passwords.
    f. Not be transmitted in the clear outside the secure location.
    g. Not be displayed when entered.

2. This agency will use advanced authentication for personnel who access and/or manage information systems containing CJI from non-secure locations. This advanced authentication is in the form of MFA.

Configuration Management

1. This agency maintains on file a detailed network configuration diagram.

Media Protection, Storage, Transport and Destruction

1. To ensure that access to digital and physical media in all forms is restricted to authorized individuals, this agency shall:

    a. Securely store all media within physically secure locations and controlled areas.
    b. Restrict access to all media to authorized individuals.
    c. Protect and control all media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
    d. Degauss or overwrite at least three times digital media before disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed.
    e. 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.

i. The destruction of digital and electronic media will be logged into an Excel database that records its media type, brand, and model, if available, what its contents were, and the destruction date. If the media had a serial number or a property\evidence number, these items shall be logged as well.
ii. Identifiable information for the digital or electronic media will be logged in the destruction CAD entry [i.e. Serial numbers and/or EXAMPLE property number]

f. Ensure all physical media is destroyed by shredding or incineration, and ensure the disposal is witnessed or carried out by authorized personnel. We have shred bins available that are covered as being able to handle and process sensitive information and ensure its confidentiality.

Physical Protection

1. This agency shall document and implement all physical protection policy requirements according to the CJIS Security Policy, to include:

a. The perimeter of the secure location shall be prominently posted and separated from non-secure locations by physical controls.
b. Issue credentials to authorized personnel or maintain a current list of personnel with authorized access to the secure location.

i. Only authorized persons are permitted access to the Pippa Passes Police Department offices.
ii. Authorized persons are those who have successfully completed security awareness training and/or CJIS User Training.
iii. Lists of authorized persons who have successfully completed CJIS user-level training and/or security awareness training are maintained and made available upon request.

c. Control physical access points by locked doors when no one is in office.
d. Control physical access to information system distribution and transmission lines within the physically secure location.
e. Control physical access to CJI on the CJIS accesses computer by:

i. Positioning computers that display and print CJIS information in such a way as to prevent unauthorized individuals from accessing and viewing CJI.
ii. Ensuring unauthorized persons do not view Information on the LINK/NCIC accessed computer.
iii. Ensuring computers with a CJIS session pulled up and logged onto are not left unsecured. However, if they are, the computer will lock after 15 minutes of inactivity.
iv. Prohibiting the use of removable storage devices in the CJIS terminal to store information from the terminal. – there is a removable policy in place.
v. Obtaining prior approval from the Chief of Police\TAC Officer before moving or relocating the LINK/NCIC terminal or printer.

f. Monitor physical access to the information system to detect and respond to physical security incidents.
g. Shall the Pippa Passes Police Department offices get visitors, they should not be left unattended, and they should not be in a area to be able to view computer screens.
h. Authorize and control information system-related items entering and exiting the physically secure location.
i. All information transmitted through LINK, NCIC, and/or NLETS shall be considered **CONFIDENTIAL** and shall be disseminated **only** for official purposes.

System and Communications Protection Information

1. The state control terminal (KSP) encrypt all network segments that access CJI with at least 128-bit NIST certified encryption to comply with the FIPS 140-2 requirements.
2. This agency will comply with the FIPS 140-2 requirements and obtain and keep on file all FIPS certificates.
3. This agency will update accordingly as the FBI CJIS Security mandates. (September 2025, **FIPS 140-6** will be standard and anything below will not be accepted)**.**

Mobile Devices

1. This agency shall authorize, monitor, and control Mobile Devices accessing CJIS systems. At the time of these policies, only the Chief of the department may use a mobile device to access the CJIS\10-8 system. All other access shall be performed on office computers.

Network Infrastructure

1. This agency will comply with CJIS Security Policy Network Infrastructure to include the following:
    a. Network Configuration- *maps and network diagrams are composed of*
    b. Personally Owned Information Systems- *Information Systems will not be personal*
    c. Publicly Accessible Computers- *computers used for CJIS will not be publicly used.*
    d. Identification/User ID- *each user has their own login for the computer and will use their own as well as their own login for CJIS*
    e. Authentication- *each user has their own login for the computer and will be authenticated against this login*
    f. Session Lock- *computers with no activity will lock after 15 minutes.*
    g. Event Logging- *all events will log to the event viewer*
    h. Advanced Authentication- access to the Information Systems require MFA
    i. Dial-up Access- *there will be no dial-up access*
    j. Mobile Devices- *the use of mobile devices shall be limited to just the chief.*
    k. Personal Firewalls – *all computers accessing CJIS will be behind a corporate firewall.*
    l. Bluetooth Access- *there will be no Bluetooth access*
    m. Wireless (802.11x) Access- *as stated in the mobile section- the only wireless access will be by the chief, and will be behind a secure firewall.*

n. Boundary Protection – *the boundaries will be protected by a firewall*
o. Intrusion Detection Tools and Techniques- *IPS is running on the firewall.*
p. Malicious Code Protection- *computers are protected from running codes*
q. Spam and Spyware Protection- *Spam and Spyware protection is covered*
r. Security Alerts and Advisories- *Security alerts are enabled per computer*
s. Patch Management- *all computers that would be used to access CJIS systems are administered by WSUS patch management.*

Misuse

1. Reports of violation of departmental, state or federal policies and regulations in regards to CJIS, CJI, NCIC, NLETS and/or LINK, misuse of CJIS equipment or information will be reported to the Chief of Police\TAC Officer.
2. Reports of violation of departmental, state or federal policies and regulations in regards to CJIS, CJI, NCIC, NLETS and/or LINK, misuse of CJIS equipment or information will be investigated in accordance with the Pippa Passes Police Department's Personnel Complaint Procedure policy
3. Persons found to be in violation of departmental, state or federal policies and regulations in regards to CJIS, CJI, NCIC, NLETS and/or LINK, misuse of CJIS equipment or information will be subject to disciplinary action in accordance with applicable policies of Pippa Passes Police Department up to and including termination

Audits and Quality Assurance

Policies and records are to be reviewed annually or more often if needed to ensure compliance with applicable statutes, regulations and policies.

This agency is aware the FBI conducts audits every three (3) years of the CSA. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

The Kentucky State Police CJIS Compliance Audit Staff will conduct, at a minimum, triennially audits on all CJAs that have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.

KSP CJIS Compliance Audit Staff can conduct unannounced security inspections and scheduled audits of all CJIS Agencies and Contractor facilities.

This agency and TAC will adhere to all guidelines of the audit process and will fully cooperate with the CJIS Audit Staff and/or the FBI and will readily make available any documentation and policy associated with any said audit.

Approved By: _____ Date: _____

Annual Review: _____, _____, _____, _____, _____, _____,

Revised: _____, _____, _____, _____, _____, _____,

APPENDIX

TERMS, DEFINITIONS and ACRONYMS:

CAD- Computer-Aided/Assisted Dispatch — A method of dispatching emergency services assisted by computer.

CHRI- Criminal History Record Information — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges

CJA- Criminal Justice Agency — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

CJI- Criminal Justice Information — Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, MC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

CJIS- Criminal Justice Information Services — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

CSA- CJIS Systems Agency — CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CSO- CJIS Systems Officer — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency. (Lt. Colonel Kentucky State Police)

CTA- Control Terminal Agency — The state criminal justice agency (Kentucky State Police (KSP) providing statewide served to criminal justice users with respect to NCIC data.

Digital Media — Any form of media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Encryption — A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort — Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

FBI- Federal Bureau of Investigation — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FIPS- Federal Information Processing Standards — Publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

(Fax)-Facsimile — Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

HIT — A computerized message received over a CJIS Terminal indicating that a person or item is entered in the LINK and/or NCIC system.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance

(ISO)-Information Security Officer — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

(III)-Interstate Identification Index — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

(IT) — Information Technology- The use of computers to store, retrieve, transmit, and manipulate data or information.

(KSP)-Kentucky State Police — The State repository agency that manages state fingerprint identification services and CJIS systems control.

(LASO)- Local Agency Security Officer — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems

(LINK)-Law Enforcement Network of Kentucky — The system, including hardware, software, equipment; facilities, procedures, agreements and organizations thereof responsible for the timely acceptance, processing, and subsequent dissemination of criminal justice.

Logical Access — The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

(MCA) Management Control Agreement — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

(MDT)- Mobile Data Terminal — A computerized device used in emergency vehicles, such as police cars, to communicate with a dispatch center.

(NCIC)-National Crime Information Center — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

(NCJA)-Noncriminal Justice Agency — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

(NICS)- National Instant Criminal Background Check System — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

(NIST)- National Institute of Standards and Technology — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

(NLETS)-National Law Enforcement Telecommunications System — Is an information sharing network. ... The NLETS helps a **law enforcement** agency in one state to search for someone's criminal and driver records in another state.

(ORI) ORIGINATING Agency Identifier — FBI authorized issued Identifier to an agency for servicing and requesting agencies CJIS information.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

(OAN) Owner Applied Number — Identification number uniquely selected from an individual of lost or stolen property to help law enforcement locate the property(s).

(PII) Personally Identifiable Information — Is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access — The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJD by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media — Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security sufficient to protect CJI and associated information systems.

Property Data — Information about vehicles and property associated with a crime.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a form information exchange agreement.

(SA) Security Addendum — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

(TAC and ATAC) Terminal Agency Coordinator and Assistant Terminal Agency Coordinator

— The TAC Serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies. The ATAC assists or fills in for the TAC when needed.

(VIN) Vehicle Identification Number — Identifying code for a specific automobile. The VIN serves as the car’s fingerprint, as no two vehicles in operation have the same VIN. A VIN is composed of 17 characters (digits and capital letters) that act as a unique identifier for the vehicle.