"Keep Orlando a safe city by reducing crime and maintaining livable neighborhoods."

ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1637.12, CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY

EFFECTIVE DATE:	5/21/2025
RESCINDS:	P&P 1637.11
DISTRIBUTION GROUP:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	CJIS AGENCY COORDINATOR
ACCREDITATION STANDARDS:	N/A
RELATED LAWS:	Fla. Stat. 943.045
RELATED POLICIES:	N/A
CHIEF OF POLICE:	ERIC D. SMITH

CONTENTS:

5. FORMS AND APPENDICES

1. PURPOSE

This directive provides procedures for the use of CJIS as FDLE has adopted the CJIS Security Policy as the standard for protecting Florida's Criminal Justice Information (CJI). The FDLE User Agreement mandates that agencies with FCIC and/or CJNet accesscomply with the CJIS Security Policy.

2. POLICY

This policy establishes guidelines for adhering to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy 6.0 and provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information (CJI) data, to protect the CJI from unauthorized disclosure, alteration, or misuse.

3. DEFINITIONS

Criminal History Record Information (CHRI) - CHRI is a subset of CJI and includes 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. This includes Computerized Criminal Histories (CCH).

Criminal History information is sensitive and should be treated as such. These records are disseminated only as a part of the user's criminal justice duties on a need-to-know, right-to-know basis. Voice transmission of a criminal history should be limited, and details of a criminal history should be given over a radio or cell phone only when an officer's safety is in danger, or the officer determines that there is a danger to the public.

The following files shall be protected as CHRI:

1. Gang Files
2. Threat Screening Center Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File. The remaining NCIC files are considered non-restricted files.

The remaining NCIC Files are considered "hot files".

Improper access, use or dissemination of CHRI and Hot File Information is serious and may result in administrative sanctions, including, but not limited to, termination of services and State and Federal criminal penalties.

Criminal Justice Information (CJI) - Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions, including, but not limited to, biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, including: fingerprints, palm prints, iris scans, and facial recognition data.

2. 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.

3. Biographic Data - information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data - information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

5. Case/Incident History—information about the history of criminal incidents. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g., within a court system presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

Criminal Justice Information Services (CJIS) - Programs within both the Florida Department of Law Enforcement (FDLE) and the Federal Bureau of Investigation (FBI) responsible for the collection, warehousing, and timely dissemination of relevant Criminal Justice Information to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Criminal Justice Network (CJNET) - A secure, private, statewide intranet system managed and maintained by the Florida Department of Law Enforcement(FDLE) to connect Florida criminal justice agencies to various data sources provided by the criminal justice community,such as secure email accounts, training manuals and announcements, memos, policy and procedure manuals, links to intelligence databases, links to State and local information systems, etc.

Florida Crime Information Center (FCIC) - FCIC is the primary system used to access Florida records, including Criminal History Record Information (CHRI), and Hot Files, which include Person, Status, and Property files. In addition, FCIC also supports queries of Concealed Weapon Permits issued by the Department of Agriculture and Consumer Services. The Concealed Weapon Permit information is for Florida concealed permits only and is provided only to law enforcement agencies.

National Crime Information Center (NCIC) - NCIC is the primary system used to access national Hot file records. Included among these records are Wanted Persons, Missing Persons, Unidentified Persons, Person Status Files, and Property Files. NCIC also allows access to the Interstate Identification Index, or III, which provides for the exchange of Criminal History Record Information between states. NCIC is maintained by the Federal Bureau of Investigation and is available to all 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, Canada, and all federal criminal justice agencies.

Personally Identifiable Information (PII) - PII is information that 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 that is linked or linkable toa specific individual, such as date and place of birth, or mother's maiden name. Any CJIS-provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record, for example, inherently contains PII as would an N-DEx case file. PII shall be extracted from CJI for the purpose of official business only. PII must be protected as required by current Stateand local statutes. There is no requirement associated with PII and secondary dissemination. PII derived from CJI should be used only for official purposes.

Personally Owned Information Systems – Any bring-your-own devices (BYOD) including cellular telephones, smartphones, smartwatches, tablets and "air cards" are examples of cellular hand-held devices or devices that employ cellular technology. Additionally, cellular hand-held devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

AGENCY ROLES AS DEFINED BY FDLE

CJIS Agency Coordinator (CAC) -The central point of contact regarding all communications between FDLE CJIS and the User. The CAC shall have User authority to ensure that all agency identified personnel, including those with decision-making authority, are made aware and able to participate in all FDLE CJIS discussions that may lead to User business and policy changes. The CAC shall have the authority to appoint other User personnel to serve in other designated CJIS positions and sign the agency contact form.

Local Agency Security Officer (LASO) and Alternate Local Agency Security Officer (Alt-LASO) - ensures compliance with the FBI-CJIS Security Policy and any other applicable security requirements. LASOs should have technical knowledge of the department's network or be able to confirm information through local technical support. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, and maintains Information Security documentation, including system and network configuration. The City's Information Security & Compliance Manager shall serve as the LASO.

FCIC Agency Coordinator (FAC) and Alternate FCIC Agency Coordinator (Alt-FAC) - ensures compliance with the legal and policy requirements contained within the CJIS User Agreement and Requirements Document, and facilitate communication between FDLE CJIS and the User regarding FCIC-related matters. The FAC/Alt-FAC should have a strong working knowledge of the CJIS systems in use by the agency and be available to respond during normal business hours.

FALCON Application Access Administrator (AAA) - creates and maintains users of the FALCON system. The AAA creates and approves users' access, provides roles and privileges to users who create and monitor Watch List records or who manage the agency's Retained Applicant Fingerprint transactions.

CJIS Online Administrator - creates and maintains CJIS Online user accounts. The CJIS Online system is used by individuals who require Security Awareness Training as mandated by the FBI CJIS Security Policy.

nexTEST Administrator - creates and maintains nexTEST user accounts. The nexTEST system contains FDLE required training for FCIC/NCIC certified operators and LASOs.

License Plate Reader (LPR) Contact - answers or relays questions specific to LPR operations at the agency.

Red Light Camera (RLC) Contact - answers or relays questions specific to RLC operations at the agency

Validations Administrator - creates and maintains user accounts within the FDLE provided online Validation Application.

4. PROCEDURES

4.1 USER AGREEMENT

The User Agreement between an agency and FDLE/FBI is a legally binding document that covers liability issues and outlines what is expected of the agency regarding proper use of FCIC/NCIC systems from that day forward. Whenever the agency head changes, the Police Legal Advisor shall prepare and submit an updated User Agreement to FDLE. The Police Legal Advisor's office shall be the central repository for these user agreements.

The agency CAC should be familiar with the contents of the agency's CJIS-related User Agreements. The CAC is responsible for notifying and ensuring that all agency users implement new CJIS procedures and capabilities when they are made available.

4.2 RELATED POLICIES

The following policies contain more detailed information on CJI:

- OPD P&P 1115, Lost or Missing Persons
- OPD P&P 1122, Police Radio Communications
- OPD P&P 1125, Report and Recovered Stolen Vehicles
- OPD P&P 1202, Filing Criminal Cases
- OPD P&P 1604, Discipline
- OPD P&P 1625, Use of Electronic Communications Systems
- OPD P&P 2301, Disposal of Sensitive Documents
- RM 600-5, Security of Criminal History Data
- City Policy 808.20, Disciplinary Action

4.3 NETWORK SECURITY

The Office of the Chief Information Officer (CIO) is responsible for maintaining the secure architecture. The FBI CJIS Security policy requires that FCIC/NCIC be encrypted to 128 bits when transmitted over a public network segment. FDLE encrypts FCIC/NCIC from the message switch to the edge routers at each agency. The City of Orlando Technology Management (or Information Technology) Division maintains a secure network architecture ensuring that all CJIS information is encrypted in transit over segments of the internal network not exclusively dedicated to Orlando Police purposes. The LASO shall maintain an up-to-date network diagram for review and audit purposes. All computers accessing FCIC/NCIC or the CJNet must have virus protection software installed and regularly updated.

4.4 FDLE CERTIFICATION REQUIREMENTS

Security and Privacy Literacy Training – required to system users as part of initial training for new users before accessing CJI, annually thereafter, as well as when there are system changes and within 30 days of a security event for persons involved in the event.

CJIS Online Training

Criminal Justice Information Services (CJIS) Security and Privacy Training

Role-based security and privacy training shall be required for all personnel who have access to Criminal Justice Information (CJI) to include personnel with unescorted access to CJIS physically secure location. Training must be completed before access is granted to agency CJI systems or information and prior to performing assigned duties. Training must be completed on an annual basis.

There are four levels of Role-based Security and Privacy Training:

- Role 1: Basic Role - for personnel who have unescorted access to a CJIS physically secure area but are not authorized to use Criminal Justice Information (CJI).
- Role 2: General Role - for personnel who are authorized to access an information system that provides access

to CJI.

- Role 3: Privileged Role - personnel authorized to perform security-relevant information technology functions
- Role 4: personnel authorized to perform security-relevant functions.

NOTE: For individuals who require Limited Access and Full Access Certification, the Role-based General User Training will be provided as part of the FCIC/NCIC Certification training and will require recertification on an annual basis.

OPD volunteers, vendors, or contract services employees who work in or visit areas where CJI is accessible must complete CJIS Online Security Certification (available in Spanish) and maintain Security Certification. This group of individuals does not have the capability to query FCIC/NCIC transactions.

All OPD personnel, Information Technology employees, OPD volunteers, and vendors who have physical or logical access to OPD computer networks with the ability to query FCIC/NCIC transactions must maintain Limited Access certification at all times. Information Technology personnel are also required to maintain CJIS Security and Privacy: Privileged Role training.

If a user lets their certification lapse, regardless of assignment, they shall not access or view CJIS data nor contact Teletype or another certified user to query CJIS information for them, as the user with the expired certificate would not be authorized to receive CJIS information. Users will receive reminders from FCIC about their certification expiring beginning 90 days before their expiration date. When a user sees this expiration notice, the certification exam should be taken as soon as possible.

FDLE will notify the agency CAC of expiring CJIS certifications.

All users requiring certification shall contact the agency CAC to arrange for the proper training.

nexTEST Online Training

FCIC/NCIC Limited Access Online Certification - The Florida Department of Law Enforcement's (FDLE) online Limited Access Certification training is for users whose job function requires queries of the Florida Crime Information Center (FCIC) and the National Crime Information Center (NCIC).

Limited Access Online Certification/Recertification Procedures:

- User must view the Limited Access online training module available on nexTEST before testing or retesting.
- User will have 14 days from the date of completing the online training module to take the Limited Access online exam.
- User must pass the 30-question exam with a score of 80% or higher. Upon passing the exam the user will be given 1 year of Security and Privacy: General User and Limited Access certification.
- A user who does not complete the Limited Access exam within 14 days of completing the online training must view the training module again prior to testing or retesting.

Limited Access Online Failure Policy:

- Users who fail the Limited Access Certification exam must retake and complete the Limited Access online training module prior to retesting.

FCIC/NCIC Full Access Online Certification - The Florida Department of Law Enforcement's (FDLE) Full Access Certification training curriculum is a combined online and classroom training designed to educate and test users in a more interactive setting. This level of Certification is for those users who will be making queries, and entries, managing record entries and conducting validations in the FCIC/NCIC system.

Full Access Certification Structure:

- Users must log into nexTEST to view the Limited and Full Access Online training modules and complete the 55-question cumulative exam to be given 6 months of Temporary Full Access certification.
- Users and agencies should plan on 3 business days for the certification exam results to be processed and the User to have access to FCIC/NCIC.
- Users must complete both online training modules (LA and FA) as well as testing for the online training within the same domain of nexTEST.
- Within 6 months of Temporary Full Access certification, the user must attend the Full Access Classroom training.
- After attending the class, the user has up to 14 days to login into nexTEST and complete the 25-question exam with a score of 80% or higher. Upon passing the exam the user will be given 1 year of Full Access certification.

To receive Full Access Certification a user must complete the following (in order):

Temporary Full Access Online Certification Procedures:

- User must view the Limited and Full Access Online training modules available on nexTEST.
- User will have 14 days from the date of completing both online training modules to take the Temporary Full Access online exam.
- User must make an 80% or better to pass the 55-question cumulative exam. Upon passing the exam, the user will be given six months of Temporary Full Access certification.
- A user who does not complete the Temporary Full Access exam within 14 days of completing the online training must view both training modules again.

Temporary Full Access Online Failure Policy:

- Users who fail the Temporary Full Access Certification exam must retake and complete both the Limited Access and Full Access Online training modules.
- Each failed Temporary Full Access certification exam will require the user to complete the above process.

Full Access Classroom Testing Procedures:

- Within 6 months of Temporary Full Access certification, the user must attend the Full Access Classroom training.
- User will have 14 days from the date of the Full Access classroom training to complete the Full Access exam via nexTEST.
- User must pass the 25-question exam with a score of 80% or higher. Upon passing the exam, the user will be given 1 year of Full Access certification.
- A user who does not complete the Full Access Classroom exam within 14 days of completing the classroom training must attend the classroom training again.

Full Access Classroom Training Failure Policy:

- A user who fails the Full Access Classroom exam must retake and complete the Full Access Classroom training prior to retesting.
- Each failed Full Access Classroom certification exam will require the user to complete the above process.
- If a user fails to attend the Full Access classroom training prior to the 6-month Temporary Full Access expiration date, the user will be denied access to FCIC/NCIC and must contact their FCIC Agency Coordinator (FAC)/nexTEST Administrator for further instructions.

Full Access Recertification Procedures:

- User must view the Limited and Full Access Online training modules available on nexTEST.
- User will have 14 days from the date of completing both online training modules to take the Full Access Recertification online exam.
- A user who does not complete the Full Access recertification exam within 14 days of completing the online training must view both training modules again.
- User must make an 80% or better to pass the cumulative 55-question exam. Upon passing the exam the user will be given one year of Full Access certification.
- A user who fails the Full Access recertification exam will be denied access and must view the Limited and Full Access Online training modules again.

Note: Users can retake the training and test as often as necessary to pass.

4.5 eAGENT

eAgent 2.0 is a web application maintained by FDLE that allows authorized personnel to make entries, inquiries, run reports, and transmit CJIS data that are in the Florida Crime Information Center (FCIC)/National Crime Information Center (NCIC) systems based upon their authority. It is fully compliant with NCIC 2000 and NLETS. This web application is compatible with most modern operating systems and web-browsers, including mobile devices, and will not require an installation.

4.5.1 AUTHORIZED eAGENT USERS

Users who are full access or limited access certified and have CJNET access may request to have an eAgent account to fulfill the law enforcement functions of that position.

4.5.2 PROCEDURE FOR REQUESTING eAgent

Any qualified employee who would like to have an eAgent account shall contact the CAC. If a user is logging into the application for the first time, they must complete the training via nexTEST and then contact their agency's CAC to receive their login credentials.

4.5.3 PROCEDURE FOR ADDING/TRANSFERRING/REMOVING eAgent

The agency CAC shall maintain a current listing of all eAgent users. The CAC will assign the user to a Team and/or Personal Inbox depending on the needs of the user.

4.5.4 REQUESTING INFORMATION FROM eAgent

The Attention (ATN) field must contain the employee identification number of the person requesting the CJIS data.

The Control (CTL) field must contain the employee identification number of the operation or employee submitting the CJIS data query.

4.6 ELVIS

The Electronic License and Vehicle Information System (ELVIS) is a web-based query-only application requiring FCIC/NCIC Limited Access certification.

4.6.1 AUTHORIZED ELVIS USERS

Authorized users must have FCIC/NCIC Limited Access certification, which shall be verified prior to the activation of an account. Users must attend an ELVIS training session scheduled and presented by an authorized ELVIS administrator. The Agency ELVIS administrator shall maintain a list of all active ELVIS accounts.

4.6.2 PROCEDURE FOR ACTIVATING ELVIS ACCOUNT

Once an employee has successfully completed the authorized user requirements, an account will be created, and the authorized user will be notified by e-mail with the account activation instructions. The instructions will include the two-factor authentication requirements which include a username and password along with the “Grid Card”. The “Grid Card” will be issued during account activation and the user will need to download and retain to access their account.

4.6.3 REQUESTING CJIS INFORMATION FROM ELVIS

All information accessed via ELVIS is permanently recorded and shall only be used for legitimate law enforcement purposes. When searching any CJIS related data via ELVIS the authorized user must complete all required fields. The “Attention” field shall be your employee number or the employee number for whom the information is being requested, and the “Reason” field shall be the case/incident number specific to the incident for which the query is being conducted.

4.6.4 PUBLIC NOTES AND COMMENTS

ELVIS allows for the addition of comments and public notes following the return of a driver license or vehicle registration check. Authorized users can add a comment for later reference that will only be visible to that authorized user. An authorized user may also elect to add a public note which can be viewed by any ELVIS user that also runs acheck on the same driver license or vehicle registration. Both comments and public notes shall only contain factual information that enhances officer safety and/or assists with a lawful investigation.

4.6.5 HIT CONFIRMATIONS

When an FCIC, NCIC, or local hit is received via mobile computer, confirmation will be obtained from Teletype via radio or telephone. Verification of any actionable CJIS related criminal history or CCW information will be obtained from Teletype via radio or telephone.

4.7 EMAIL

Emailing CJIS-related material is prohibited using the City’s email system as it does not currently meet CJIS Encryption standards. (FBI Security Policy Encryption shall be a minimum of 128 bit.) Additionally, employees shall adhere to the procedures outlined in the current issue of City P&P 754.11, E-mail.

The Florida Department of Law Enforcement (FDLE) provides a secure electronic mail service to criminal justice agencies throughout the state of Florida. This service complies with CJIS encryption standards, ensuring the safe transmission of sensitive information.

To request a CJNET email address, visit https://flcjn.net/Email. A CJNET email account enables authorized users to securely send and receive criminal history records via encrypted email.

4.8 DATA STORAGE

UNIVERSAL SERIAL BUS (USB) DEVICES (FLASH/THUMB /EXTERNAL DRIVES)

CJIS Data is prohibited from being stored on either City or personal USB devices.

PRINTERS

A printer is defined as an electronic device capable of buffering the information only long enough to print. Information is not stored long-term on this machine. CJIS data is prohibited from being printed on devices outside the Orlando Police Department.

MULTI-FUNCTIONAL DEVICES

A multi-functional device is a copier, printer, scanner and/or fax machine capable of storing information long-term. The disposal process for this machine should be treated the same as if it were a computer. CJIS data is prohibited from being printed on multi-functional devices outside the Orlando Police Department.

CLOUD CJIS FCIC/NCIC

Employees are prohibited from transmitting or storing data on any Cloud solution without the approval of the City Local Agency Security Officer (LASO). Cloud solutions include Google apps (email, Google Docs, Google Sites), Facebook, etc. (see Appendix A), as those solutions do not currently meet CJIS encryption standards.

NETWORK DRIVE

Criminal history records may be requested for storage on the N Drive. Once processed by Teletype, the records will be placed in the "CRIMINAL HISTORY" folder at: *N:\OPD\COMMON_CRIMINAL HISTORIES.* This is a secure location, protected by a firewall to ensure data security. Criminal histories must only be stored within N:\OPD and should not be placed elsewhere.

4.9 FAXING

Faxing CJIS-related material is prohibited without first being authorized by the Department's CAC.

4.9.1 TRANSMITTING CRIMINAL HISTORIES VIA FACSIMILE (FAX) MACHINE

Teletype operators shall not routinely transmit via facsimile (fax) machine any criminal history data obtained from FCIC/NCIC, unless there is an immediate need to further an investigation or there is a situation affecting the safety of the officer or the general public. Histories may be transmitted by facsimile upon approval of the agency CAC. Fax machine location and potential access from non-CJIS-certified personnel or the public is the determining factor for approval. Per FDLE, histories may be faxed to any location with an ORI. Histories may be faxed to all Orlando Police Department substations, including the Orlando International Airport, with an accompanying fax cover sheet. Officers receiving faxed histories must advise the Teletype operator that they have received the fax. This notification may be made via the radio or on the phone. When in doubt about faxing a history to a location, users shall contact the agency CAC. If the receiving party faxes the information to another agency with an ORI different from that of the Orlando Police Department, this dissemination must be recorded on OPD ONLINE CJIS logs, Secondary Dissemination.

4.10LOGGING AND DISSEMINATION OF CJI

Users are required to log all Criminal Histories they run and/or information they disseminate to persons outside the ORI: FL0480400 assigned to the Orlando Police Department. Users may access the Criminal History Record Information Requests Verification Form and the Secondary Dissemination Form from the CJIS logs link available on OPD Online. Users should contact the agency CAC with questions regarding the CJIS logs or if data entered needs to be amended or deleted.

LOGGING CRIMINAL HISTORY REQUESTS

Members will provide specific reasons for each inquiry (e.g., OPD case number or burglary investigation, expungement of record, private contractor, employment check, file maintenance, sex offender registration, etc.).

LOGGING SECONDARY DISSEMINATION

When the person requesting and/or in the possession of the criminal history shares any part of that information with another criminal justice professional outside of their agency, either *physically or verbally*, that action is considered secondary dissemination and must be recorded in the OPD Online CJIS logs located on the main page of OPD ONLINEor under the Admin/Logs.

The purpose of the Secondary Dissemination Log is to provide an audit trail and list all persons having direct access to the criminal history record. This log must be maintained at the agency for at least four years for audit purposes. The following information shall be annotated in the log: Date the Criminal history was released, Subject's Name, SID/FBI Number, Requestor name (who the information was released to), Employee# or Badge# if applicable, Agency name, Related case Number, Purpose Code used to run criminal history, Name of person releasing information, and Reason Disseminated (*OPD case number, or associated case investigation)* Records of Criminal History queries and dissemination will be requested by both the FBI and FDLE during triennial (every three years) agency audits. All case packages transmitted to the State Attorney's Office that include a criminal history require an entry in the secondary dissemination log. Periodic internal agency audits may be conducted to ensure compliance with the above-referenced policy.

DISSEMINATION OF COMPUTERIZED CRIMINAL HISTORY (CCH) WITH AFFIDAVIT OF PROSECUTIVE SUMMARY (APS)

When submitting an APS that requires a criminal history to be run and included with the APS package, the officer writing the APS shall run and log the Criminal History in the Secondary Dissemination Log in the CJIS logs link availableon OPD Online, noting that it will be disseminated to the State Attorney's Office (OPD Policy 1202, Filing Criminal Cases).

PUBLIC RECORD REQUEST

Public Record requests for Teletype transactions or information obtained from the FCIC shall not be made available to non-criminal justice agencies or private individuals unless specifically authorized by statute. Information derived from the FCIC, including criminal history information, shall not be made available under Florida's Public Record Law (F.S. 119). Requests for FCIC information from non-criminal justice agencies, or individuals, must be made directly to the Florida Department of Law Enforcement. Information on filing a public records request can be found at www.fdle.state.fl.us.

4.11DISPOSAL

DISPOSAL OF HARDCOPY CRIMINAL HISTORIES

Criminal history data is constantly changing and should be kept only until a case file is closed or the record is superseded, obsolete, or the administrative value is lost. Criminal histories should not be retained in case files: if a history is needed at a later time, a new history should be obtained. Criminal histories in the box in Teletype should be sorted through on a nightly basis. All criminal histories that have been held for ten days should be shredded. When destroying a criminal history record, agencies are required to dispose of it in a secure manner by shredding or burning the document(s). It is not to be discarded in the trash. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel. Documents that have not lost their value and are still being kept for investigative purposes must be kept in a manner to prevent unauthorized or unintended access.

DISPOSAL/DESTRUCTION OF ELECTRONIC MEDIA

Electronic media used to store FCIC/NCIC must be properly erased/sanitized/wiped prior to disposal (disposal includesreuse by or transfer to a non-criminal justice entity). Electronic media includes, but is not limited to, diskettes, tape cartridges, ribbons, CDs, DVDs, digital memory cards, external hard drives, hard drives from computers and USB flash drives. FDLE encourages physical destruction of storage media prior to disposal. If the media is not physically destroyed, it must be completely overwrittenat least six times to prevent unauthorized access to the previously stored data. In situations where computers are moved **within** an agency from an FCIC user to a non-FCIC user, all FCIC-related files should be removed from the device prior to reallocation to the new users. Additionally, all hardware and storage media should be erased/sanitized/wiped prior to surplus or transfer within the criminal justice agency. Please reference OPD Policy 2301, Disposal of Sensitive Documents, for more details on this disposal procedure.

4.12AUDITS

FLDE AUDITS

FDLE Auditors conduct triennial (every three years) audits in compliance with Florida Statute 943 on every agency with access to the CJNet and FCIC/NCIC. Audits consist of an on-site visit by the audit staff. At the discretion of the auditors, an on-site visit can be performed at an agency regardless of the entry/non-entry status of that agency. The objective of the audit is to verify adherence to CJIS policies and procedures.

During an on-site visit, FDLE auditors will use a questionnaire to evaluate entries in the system and a sample of these entries will be checked for accuracy and proper validation procedures. The auditor will also need to review any

Interagency User Agreements currently in use by the agency, perform a technical audit (overseen by the LASO) and review a network diagram. An out-briefing will be conducted, and any violations, potential problems, or recommendations will be identified, followed by a written report sent to the agency head. If an agency is cited with a violation, the agency must respond, in writing, within thirty (30) days identifying corrective measures taken to ensure compliance.

FBI AUDITS

The FBI CJIS Division is authorized to conduct a triennial (once every three years) audit as a minimum to assess agency compliance with applicable statutes, regulations, and policies. Audits may be conducted on a more frequent basis if the audit reveals that an agency is not in compliance. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CJI APPLICATION AUDITS

In accordance with FBI CJIS Security Policy, audit logs must be captured for every Criminal Justice Information (CJI) system and application utilized by OPD personnel.

AUDIT LOG REQUIREMENTS FOR CJI SYSTEMS AND APPLICATIONS

- If OPD hosts the system/application servers, OPD is responsible for ensuring all required audit events are captured.
- If the system/application servers are hosted by an external entity or agency, OPD's responsibility is limited to reviewing the audit logs.

Regardless of where the servers are hosted, **audit logs for all CJI applications and systems must be reviewed on a weekly basis.**

AUDIT LOG REVIEW AND COMPLIANCE

FDLE does not mandate specific documentation of audit log reviews for compliance. Instead, compliance is determined based on the designated personnel responsible for log review and their ability to consistently access and assess logs.

REQUIRED AUDIT LOG EVENTS

Audit logs must capture the following events:

- Successful and unsuccessful log-on attempts
- Successful and unsuccessful attempts to access, create, write, delete, or modify permissions on a user account, file, directory, or other system resource
- Successful and unsuccessful attempts to change account passwords
- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, *and* destroy the audit log file
- The type of event that occurred
- Date, time, and location of the event
- The source of the event
- The outcome of the event
- The identity of any individuals, subjects, or objects associated with the event
- The session, connection, transaction, and activity duration
- The source and destination addresses
- The object or filename involved

- The number of bytes received and bytes sent in the audit records for audit events identified by type, location, or subject

AUDIT LOG DOCUMENTATION & ACCOUNTABILITY

To ensure accountability, the CJIS Agency Coordinator (CAC) maintains a **OneDrive file** for tracking audit log reviews. Each **CJI Administrator** responsible for performing weekly audits must document their reviews in this log.

4.13MEMORANDUMS OF UNDERSTANDING

Any Memorandum of Understanding entered into with the FBI, FDLE, or another Law Enforcement Agency should be reviewed in its entirety by the Police Legal Advisor's officer. The Police Legal Advisor's office shall be the central repository for these agreements.

4.14VIOLATIONS

Misuse or violations of this policy shall be addressed in accordance with the current issue of Orlando Police Department Policy and Procedure 1604 Discipline, and City Policy and Procedure 808.20 Disciplinary Action unless FDLE chooses to pursue criminal proceedings.

The following are some examples of misuse and would be a violation of the User Agreement with FDLE as well as this policy:

- Use of fingerprint scanner to assist a hospital in identifying an unknown patient who is not otherwise involved in a criminal investigation
- Running a criminal history background check on an individual in preparation for a civil injunction hearing
- Accessing criminal history information for any civil landlord-tenant issue
- Employment verification for non-law enforcement personnel

4.15DEVICE SECURITY

MCT users shall close the lid of their computer when exiting the vehicle with the computer on to prevent non-CJIS-certified members or citizens from viewing data on their screen.

4.16CUT, COPY, AND PASTE OF CJIS MATERIAL

An agency must meet the requirements of the FBI CJIS Security Policy prior to cutting and/or copying and pasting from an FCIC/NCIC response (this would include any transaction received from the FCIC message switch) into a local system. Local systems include email, record management systems, jail management systems and any type of electronic storage media that is accessed via a network connection. Members shall not cut and/or copy and paste FCIC/NCIC and CHI responses into City email or personal email.

4.17PERSONALLY OWNED INFORMATION SYSTEMS

Personally owned information systems shall not be authorized to access, process, store or transmit Criminal Justice Information until the Department has established and documented the specific terms and conditions for personally-owned information system usage. When bring-your-own devices (BYOD) are authorized, they shall be controlled using the requirements of an approved Mobile Device Management (MDM) system and of the FDLE CJIS Security policy. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the Department.

This control does not apply to the use of personally owned information systems that access the City of Orlando information systems and information that is intended for public access (e.g., the City's public website, which contains purely public information).

4.18NATIONAL RAP BACK

OVERVIEW:

The Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) Noncriminal Justice Rap Back Service ("National Rap Back") was designed to provide the agency with national notifications when the following triggering events occur:

- Criminal Arrests
- Want Additions and Deletions (new warrant entry which includes the individual's FBI/UCN number)
- Sexual Offender Registry Additions and Deletions
- Death Notice with Fingerprints

If a triggering event occurs with a retained applicant, the agency's CJIS Agency Coordinator, Alt FAC, and ID Unit will be notified via the Florida Department of Law Enforcement's (FDLE) Information Notification System (FINS).

AGENCY RESPONSIBILITY:

The FBI Criminal Justice Information System (CJIS) Security Policy requires fingerprint-based record checks to be conducted **prior** to granting access to criminal justice information (CJI) or areas where CJI is handled or processed (secure areas). Applicants are given the Applicant Notification and Acknowledgement Form on paper to read and sign. Fingerprints submitted by applicants will be retained by the Florida Department of Law Enforcement (FDLE) and the Federal Bureau of Investigation (FBI) as part of the National Rap Back Service. The agency is required to maintain FALCON user accounts to ensure compliance with the required background check provisions of the FBI Criminal Justice Information System (CJIS) Security Policy and Florida State Statute. Additionally, the agency is responsible for removing retained applicant fingerprints of any person for which the agency is no longer authorized to receive criminal history information (i.e., upon member separation) within five (5) business days.

ANNUAL VALIDATION :

The FBI requires that all subscriptions (i.e., retained applicants) have an expiration or validation date as part of National Rap Back's privacy risk mitigation strategies. Criminal Justice agencies' retained applicants are lifetime enrollments; this means that the applicant will continue to be retained at the state and national level until the applicant is deleted from FALCON. Therefore, agencies are required to validate these subscriptions annually, which refers to deleting or affirming the subscription is still valid and that the agency continues to have the relationship entitling the agency to receive notifications.

NOTICE TO APPLICANTS/CURRENT AGENCY PERSONNEL:

This notice is to inform applicants and current agency personnel that a fingerprint-based record check will/has been conducted for all individuals seeking employment with the Agency. The purpose of the records check is to conduct a search of any Florida and National criminal history records that may pertain to the applicant/employee. By submitting fingerprints, you are authorizing the dissemination of any state and national criminal history record that may pertain to you to the agency from which you are seeking employment. The fingerprints submitted are retained by the Florida Department of Law Enforcement (FDLE) and the Federal Bureau of Investigation (FBI). The fingerprints will be retained with the agency until such time as employment separation occurs. In the event of subsequent arrests, FDLE and the FBI will notify the agency of a records hit based on those retained fingerprints.

If you believe that the criminal history record is incomplete or inaccurate, you may conduct a personal review as provided in s. 943.056, F.S., and Florida Administrative Code Rule 11C-8.001 by calling FDLE at (850) 410-7898. If you believe the national information is in error, you may contact the FBI at (304) 625-2000. You can receive any national criminal history record that may pertain to you directly from the FBI, pursuant to 28 CFR Sections 16.30-16.34. You have the right to a reasonable amount of time to obtain a determination as to the validity of your challenge before a final decision is made about your status as an employee, volunteer, contractor, or subcontractor.

4.19CJIS ACCESS REVIEW

Per Federal Bureau of Investigations, CJIS Security Policy, and the FDLE Criminal Justice User Agreement Section III, agencies are required to properly vet individuals before granting unescorted access to unencrypted CJI or to physically secure areas where CJI is handled, processed, or stored. If an individual with established access is subsequently arrested, charged, or convicted of a criminal offense, access to CJI shall be denied, and an access review request submitted to FDLE. Future access to CJI shall be determined by the FDLE CJIS Systems Officer (CSO). This form shall be submitted to the CSO to request a review when persons with physical or logical unescorted access, or being considered for a position requiring access, are found to have a criminal record of any kind.

The CJIS Agency Coordinator will submit the Review Access Request Form FDLE and notify via Chain of Command.

5. FORMS AND APPENDICES

APPENDIX A-Cloud Solutions

APPENDIX B- CJIS Guidelines