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

ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1637.8, CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY

EFFECTIVE:	10/15/2021
RESCINDS:	1637.7
DISTRIBUTION:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	TERMINAL AGENCY COORDINATOR
ACCREDITATION STANDARDS:	NONE
CHIEF OF POLICE	ORLANDO ROLÓN

CONTENTS:

POLICY:

This policy establishes guidelines for adhering to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy 5.0 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. 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 access comply with the CJIS Security Policy.

PROCEDURES:

1. DEFINITIONS

1.1 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.

1.2 FLORIDA CRIME INFORMATION CENTER (FCIC)

The State of Florida's centralized database for tracking crime-related information, which can be queried by appropriate Federal, State and local law enforcement and other criminal justice agencies.

1.3 NATIONAL CRIME INFORMATION CENTER (NCIC)

The national centralized database for tracking crime-related information, which can be queried by appropriate Federal, State and local law enforcement and other criminal justice agencies.

1.4 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.

1.5 CRIMINAL JUSTICE INFORMATION (CJI)

The term used to refer to all CJIS-provided data, either from the FBI or FDLE, necessary for law enforcement agencies to perform their missions and enforce the laws, including, but not limited to, biometric, identity history, biographic, property, and case/incident history data. CJIS FCIC/NCIC data is provided to criminal justice agencies and statutorily defined agencies for official criminal justice purposes. The term "criminal justice purpose" is defined in section 943.045(2), Florida Statutes, and 28 Code of Federal Regulations (CFR) Part 20.3 as follows: “Administration of criminal justice means performing functions of detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders by governmental agencies. The administration of criminal justice includes criminal identification activities and the collection, processing, storage, and dissemination of criminal justice information by governmental agencies.” FDLE has adopted the FBI CJIS Security Policy as the foundation for FCIC, CJNet, Interstate Identification Index (III) and Computerized Criminal History (CCH) records related to information security. FCIC/NCIC data is any data obtained through a query to the FCIC message switch or other systems accessed via the CJNet (excluding DAVID), containing FCIC/NCIC Hot Files, Florida CCH and/or III/CCH information from other states and/or the FBI. Any information from an FBI system (NCIC, III, N-DEX) or FCIC or Florida criminal history record shall be considered CJI.

1.6 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 File
2. Known or Appropriately Suspected Terrorist File
3. Convicted Persons on Supervised Release File
4. Immigration Violator File (formerly the Deported Felon File)
5. National Sex Offender Registry File
6. Historical Protection Order File of the NCIC
7. Identity Theft File

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.

1.7 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 to a 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 State and local statutes. There is no requirement associated with PII and secondary dissemination. PII derived from CJI should be used only for official purposes.

1.8 CJIS AGENCY COORDINATOR (CAC)

The CAC is responsible for ensuring agency and user compliance with CJIS policies and procedures as they relate to FCIC and NCIC. The CAC is designated by the Chief of Police and serves as the point-of-contact for matters relating to CJIS information access.

1.9 LOCAL AGENCY SECURITY OFFICER (LASO)

The 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 his or her agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to his or her constituents, and maintains Information Security documentation, including system and network configuration. The City's Technology Management Security Officer shall serve as the LASO.

1.10 PERSONALLY-OWNED INFORMATION SYSTEMS

Any bring-your-own devices (BYOD) including cellular telephones, smartphones (Blackberry, iPhone, etc.), personal digital assistants (PDA), 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.

2. 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.

3. 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	REPORTED 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
OPD	RM 600-5	SECURITY OF CRIMINAL HISTORY DATA
CITY	Policy 808.20	DISCIPLINARY ACTION

4. 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.

5. FDLE CERTIFICATION REQUIREMENTS

Personnel who have written, computerized or audible access to CJI data will require either Full or Limited Access CJIS certification and/or CJIS Online Security certification within six months of initial assignment, and biennially (every two years) thereafter.

CJIS Online Security Certification is obtained by personnel reviewing online instruction offered by FDLE. This instruction will conclude with personnel taking a 25-question test administered by the software program. Users must pass the test with a score of 80% or greater. A score of less than 80% will require the user to retake the online instruction. Upon completion users can print a certificate; they will understand how to properly handle CJIS-related information and will be granted query access only to CJIS-related data.

For Existing Full Access Certified Users:
Existing entry operators are required, upon expiration of their current FCIC/NCIC Full Access Certification, to participate **one time** in the new Full Access certification process. After the January 2016 launch, current Full Access Users are required to take the new Full Access training flow and exams within 120 days of their current Full Access certification expiration.

For New Full Access (FA) Certifying Users:

1. Online Training in nexTEST
    a. New FA Users must complete Limited access Online Certification module
    b. New FA Users must complete Full Access Online module
    c. Successfully pass a comprehensive (50) question online exam, with a passing score of 80% or higher, within fourteen (14) days of completing both online modules
    d. User will automatically receive six (6) months of Temporary Full Access to FCIC/NCIC
2. Classroom Instruction
    a. New FA Users must participate in a Full Access Classroom instruction prior to the end of the six (6) months of Temporary Full Access
    b. Successfully pass a twenty-five (25) question online exam, with a passing score of 80% or higher, within fourteen (14) days of classroom instruction
    c. User will receive two (2) years of Full Access Certification

Future Re-Certification for Full Access:

Following the two-year expiration cycle, and current user participation in the online and classroom instruction, future re-certification shall be performed online as follows:

a. Re-certifying FA Users must complete the Limited Access Online Certification module

b. Successfully pass a comprehensive fifty (50) question online exam, with a passing score of 80% or higher

Future Full Access Expiration Procedures:

If a user allows his or her Full Access certification to expire, access to the system is immediately denied. To regain access the user must:

a. Complete the Limited Access Online Certification module
b. Complete the Full Access Online module
c. Successfully pass a comprehensive fifty (50) question online exam, with a passing score of 80% or higher

Future Full Access Failure Procedure:

1. Online training Failure:
   a. User is locked out of FCIC/NCIC
   b. Upon failure of the modular training exam a user must go back through both the Limited Access and Full access online training. Upon completion of re-training, the user must contact their Terminal Agency Coordinator (CAC)/ nexText administration who will request the regional IDT Member or Customer Support Center (CSC) to unlock the user in nexTest so the user may retest.
   c. Each failure will cause the user to complete the above process. A user will have three opportunities to pass the exam. The third failure will result in a user's inability to be certified as a Full Access operator for a period of one (1) year.

2. Classroom training Failure:
   a. User is locked out of nexTest and FCIC/NCIC
   b. If the failure occurred less than 180 days from attending classroom instruction user may be registered for classroom training again and retest.

If the failure occurred more than 180 days from attending classroom instruction, the CAC must contact FDLE to have the user reset in the nexTest system. User will have to view the Limited Access and Full Access Online training again and retest, then register and attend classroom training again and retest.

Limited Access Training:

a. Follow the 'Limited Access Certification Training Link' provided and log in to nexTEST.
b. A user will authenticate to nexTEST with his/her login credentials. Within nexTEST choose the 'Training' Tab and select the 'Begin Training' button. *Note: Due to local Internet/CJNet connectivity some users may periodically experience slowness in loading the training.*
c. Upon completion of the training module the final slide will provide the nexTEST icon, which the user must click on to be re-directed back to the nexTEST application. The user may begin the Limited Access Certification test immediately.
d. Users must complete testing within the same domain that the initial login to nexTEST and training occurred. (Example: If a user initiates training on CJNet, testing must occur on CJNet.)
e. If you are not able to complete the exam immediately following the training, you will have 14 days to log back into nexTEST and complete the exam. You must receive a score of 80% or higher

Limited Access Training Failure:

a. If you fail the exam you will not be shown the correct answers and are required to view the online training again and retest.
b. Upon completion of re-training contact your CAC or nexTEST administrator who will verify the retraining has been completed and then will contact FDLE CJIS to unlock the test.
c. After the test has been unlocked and then you will be able to retest.
d. If you fail the exam three times in a one year period you will not be allowed to re-train and test for one year from the last failed attempt. Additionally, you will be denied access to FCIC/NCIC.

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, or 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 CJIS certification at all times. Information Technology personnel are also required to maintain CJIS Online level 4 security 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 prior to their expiration date. When a user sees this expiration notice, the certification exam should be taken as soon as possible. Users who allow their certification to remain expired for two years or more will be required to attend classroom training.

FDLE will notify the agency CAC of expiring CJIS certifications. The CAC shall disseminate this list to both sworn and civilian training coordinators and the agency LASO who shall send email notifications of upcoming expirations to the individuals with expiring certificates.

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

6. eAGENT

The FCIC eAGENT system is a browser-based application provided and maintained by FDLE that allows CJIS certified users to query, enter, modify, locate, clear and cancel records that are in the Florida Crime Information Center (FCIC II)/National Crime Information Center (NCIC2000) systems based upon their user authority. The purpose of this software for most users is to run criminal histories.

6.1 AUTHORIZED eAGENT USERS

This software can be loaded onto any desktop, laptop or mobile computer used by Law Enforcement personnel. Users with full CJIS certification and a qualified OPD computer may request to have eAGENT installed on their computer to fulfill the law enforcement functions of that position.

6.2 PROCEDURE FOR REQUESTING eAGENT

Any qualified employee who would like to have eAGENT loaded onto their computer shall contact the Information Technology Help Desk who, in turn , shall contact an Information Technology Business Analyst. who will request a mnumoic from the Agency CAC.

6.3 PROCEDURE FOR ADDING/TRANSFERRING/REMOVING eAGENT

The agency CAC shall maintain a current listing of all devices assigned with eAGENT mnemonics and shall notify the Technology Management Business Analysts when eAGENT is to be added or removed from an authorized device.

6.3.1 eAGENT EXCEPTIONS

Authorized eAGENT users with a mobile computer (for example, a Criminal Investigations Division detective) shall not, under any circumstances, take their assigned mobile computer with them when transferred to Patrol, Downtown Bikes, or any other work unit where the computer will not be docked in a desktop docking station 80% of the time. At no time shall a mobile computer with eAGENT on it be utilized in a patrol vehicle. Any user found to be violating this directive shall face disciplinary action, as this violates the agency User Agreement and could jeopardize the Agency's access to CJIS data.

6.4 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 operator or employee submitting the CJIS data query.

7. ELVIS

The Electronic License and Vehicle Information System (ELVIS) is a web-based

query only application requiring either Full or Limited Access CJIS certification and/or CJIS Online Security certification.

7.1 AUTHORIZED ELVIS USERS

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

7.2 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 includes 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.

7.3 REQUESTING CJIS INFORMATION FROM ELVIS

All information accessed via ELVIS is permanently recorded and shall only be used for legitimate law enforcement purpose. 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, the “Reason” field shall be the case/incident number specific to the incident for which the query is beingconducted.

7.4 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 a check 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.

7.5 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.

8. EMAIL

Emailing CJIS-related material is prohibited as the City’s email system 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.

9. DATA STORAGE

9.1 UNIVERSAL SERIAL BUS (USB) DEVICES (FLASH/THUMB /EXTERNAL DRIVES)
CJIS Data is prohibited from being stored on either City or personal USB devices.

9.2 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.

9.3 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.

9.4 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.

10. FAXING

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

10.1 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 when 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.

11. LOGGING 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 and the Secondary Dissemination logs 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.

11.1 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.).

11.2 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 ONLINE or 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 and time of request; name of subject whose history was run; SID # or FBI # of subject; name of employee or person requesting the criminal history; the agency to which the information was released; employee number of operator making the query; the reason the information was disseminated; the purpose code; case number (if applicable); and any additional notes. 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.

11.3 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 available on OPD Online, noting that it will be disseminated to the State Attorney's Office (OPD Policy 1202, Filing Criminal Cases).

110.4 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.

12. DISPOSAL

12.1 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.

12.2 DISPOSAL/DESTRUCTION OF ELECTRONIC MEDIA

Electronic media used to store FCIC/NCIC must be properly erased/sanitized/wiped prior to disposal (disposal includes reuse by or transfer to a non-criminal justice entity). Electronic media includes, but is not limited to, diskettes, tape cartridges, ribbons, CDs, DVDs, 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 overwritten at 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.

13. AUDITS

13.1 FDLE 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.

13.2 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.

13.3 DAVID AUDITS

The Department of Highway Safety and Motor Vehicles (DHSMV) requires an in-person audit every two years to review and assess agency compliance with applicable statutes, regulations and policies. A random inspection of user's activity will be reviewed for compliance. Those serving as point of contacts shall conduct a quarterly self-audit and retain the results.

13.4 FINDER and ELVIS AUDITS

The Florida Department of Law Enforcement (FDLE) Information Technology Audit and Compliance section has determined FINDER and ELVIS services require an annual user audit certifying all the agency's users are currently employed by the Orlando Police Department. An assigned administrator shall, on a weekly basis, conduct and document review audit logs to identify any possible misuse of the system.

14. MEMORANDUMS 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 office. The Police Legal Advisor's office shall be the central repository for these agreements.

15. VIOLATIONS

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

16. DEVICE 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.

17. CUT, 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 Google email or personal email.

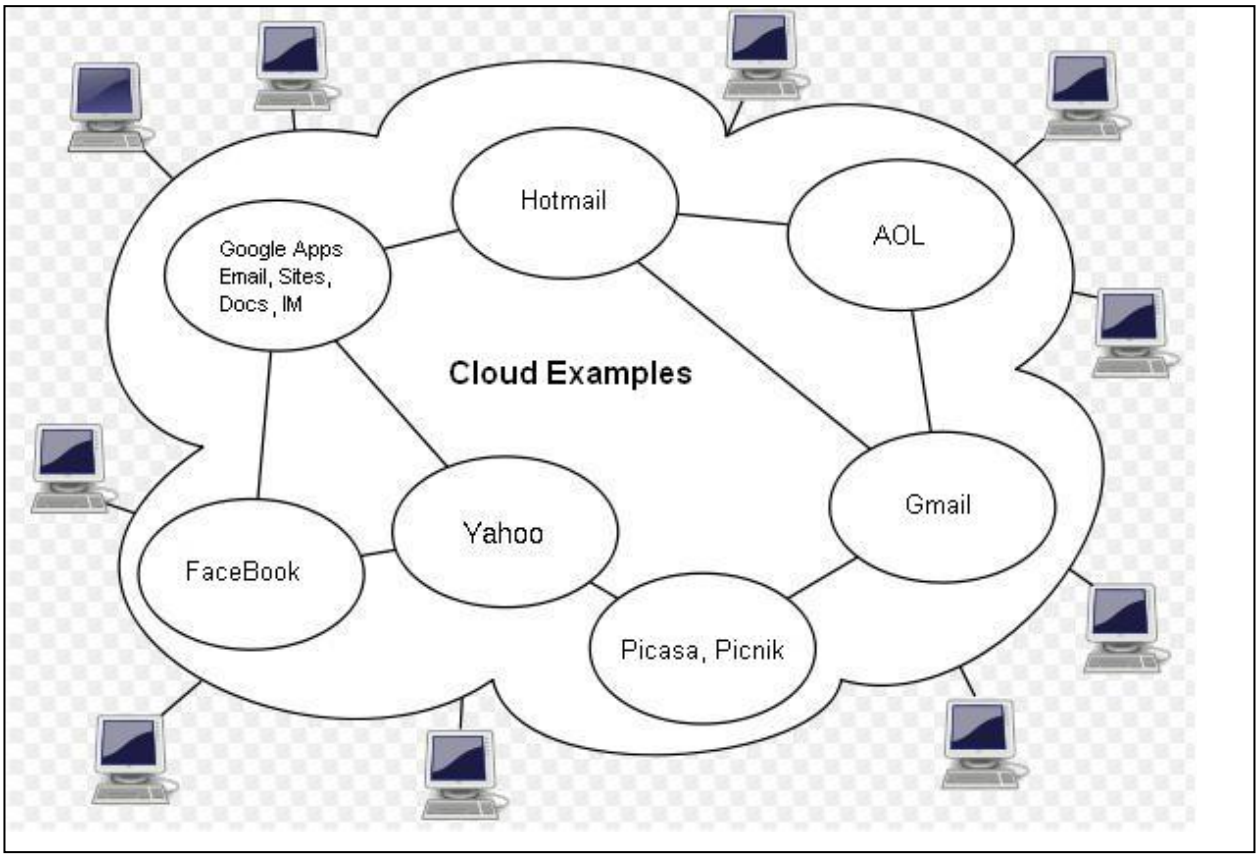
18. PERSONALLY-OWNED INFORMATION SYSTEMS

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).

Appendix A

CLOUD SOLUTIONS



Emailing, transferring, storing, or copying/pasting any portion of CJIS FCIC/NCIC-related material to Solutions in the Cloud is prohibited unless approved by the City Local Agency Security Officer (LASO).

Appendix B

REQUIRED POLICES FOR CJIS COMPLIANCE

The overriding goal of the following policies is to comply with the Federal Bureau of Investigations (FBI) Criminal Justice Information Systems (CJIS) Security Policy and the Florida Department of Law Enforcement (FDLE) User Agreement requirements. Due to the evolving nature of the CJIS Security Policy (CSP), it is necessary to separately communicate the requirements of the CSP Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Orlando Police Department (OPD), CJIS Policy.

PERSONALLY, IDENTIFIABLE INFORMATION

Definition:

PII Personally Identifiable Information (PII) 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. Any NCIC or FCIC provided data maintained by OPD, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include an individual's PII.Collection

- All PII will be collected only when there is a legal authority and it is necessary to conduct OPD duties. Access to PII is only conducted when the information is needed to conduct OPD official duties and should only be utilized for official purposes. OPD employees will not create duplicate copies of documents that contain PII and will destroy the documents when no longer needed. When PII is extracted from a document OPD employees member may only target the PII that is required for the task. PII that is extracted shall not be retained beyond the records retention rules for the data and the system it was accessed from. PII shall not be stored or transmitted via personally owned devices. PII may not be taken home by any OPD employee member.

Storage

- All electronic files that contain PII are stored in network folders secured by controlled access. All physical files that contain PII reside in the Orlando Police Department Records Section, restricted from public access. Electronic media containing CJI or PII must be encrypted before it is moved outside of a secure location. Once moved outside a secure location on removable media, PII must be locked in a designated physically secure location

Disposal

- Disposal of physical PII, shall be in locked blue storage bins to be shredded, bins are provided to each Department /Division, in restricted locations, without public access. disposal of CJI OR PII will be done by authorized OPD personnel.

Transfer

- PII is not permitted to be downloaded to workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the OPD. PII will also not be sent through any form of insecure electronic communication as significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted. All disposal of PII will be done by authorized OPD personnel.

INFORMATION EXCHANGE

Definition:

Criminal Justice Information is the term used to refer to all 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. CJI is considered any information that is derived from NCIC and/or FCIC and should be treated as such. OPD will put forth formal agreements with other agencies prior to exchanging criminal justice information as well as the use of secondary dissemination.

Sharing CJIS Information

- OPD allows for criminal justice information to be shared with local law enforcement agencies and has current agreements in place with each. This exchange is allowed only via hard copy as well as shared CJI applications.

Logging Dissemination

- All OPD employees have virtual access to both CJIS Logs. The logs denote the employee who ran Criminal History Record Information (CHRI) and the employee who requested the CHRI information. The CJIS Secondary Dissemination Logs must be completed If an employee needs to share CJI with another agency that it does not currently have an agreement with, another Agency the Agencies Secondary Dissemination Log must be completed. All Disseminated Criminal Justice Information (CJI) shall be documented in the

dissemination log including: date, subject's name, SID or FBI number, requestor, requestor agency, operator, reason disseminated, and purpose code.

INFORMATION HANDLING

Definition

Information obtained from the CJI systems, must only be used for criminal justice purposes. Personnel must follow all CJIS Security Policy, state and federal rules and regulations regarding CJI information. All personnel with access to CJI, audio as well as visual, shall receive the proper training within 30 days of hire. CJI or Personally Identifiable Information (PII) will not be transmitted via email unless it meets the encryption requirements of the CSP. All information outlined in the information exchange and disposal of physical media shall be followed as well. These procedures shall include all inquiries for both criminal justice and non-criminal justice purposes.

Storage

- OPD utilizes servers for storage of criminal justice information. The servers are kept in a physically secured building inaccessible to non-authorized individuals. The doors have key card locks that are only accessible to OPD employees. All physical files that contain CJI reside in the Orlando Police Department Records Section, restricted from public access. Physical information, such as reports that contain criminal justice information in the records Department that is only accessible to OPD personnel. The documents are stored in a secured area within the room and are only removed when needed for operational purposes. When removed, the information is kept by an authorized individual and then returned. The removal is documented in a log.

Transport/ Transmitting

- Any information that must leave OPD facility for transport will be done so only by authorized personnel and only for operational purposes. OPD does not allow CJI to be transmitted via email.

Unauthorized Viewing

- All computers within the agency must be turned away from view to prevent unintentional viewing or shoulder surfing.

INCIDENT RESPONSE

Definition

To ensure protection of CJI, OPD and Information Technology (IT) has created the following incident response policy. The policy covers procedures that include preparation, detection, analysis, containment, recovery, and user response activities to an incident as well as the administrative duties of tracking, documenting, and reporting of incidents to the appropriate authorities as required.

Compromising Incident

- Any employee who suspects that an information security incident occurred, shall immediately contact the IT Help Desk at 407-246-2400. The Help Desk will document the events related to the misuse or compromise of CJIS/FCIC/NCIC. The incident to the Local Agency Security Officer (LASO). The LASO will manage the breach based on the level of severity of the incident and will notify FDLE. User accounts will be disabled upon first discovery of compromise.

Mobile Devises

- If a suspected incident occurs on an agency mobile device, the user shall not turn off the device. The user will leave the device on and immediately report the incident to the IT Help Desk who will examine the device and determine if the incident is contained to the one device or if it is within the Agency system.

Documentation

- The LASO and Security Team will review all security incidents on a weekly basis ongoing basis and will retain documentation until it is no longer needed for audits and/or if legal action.

ACCOUNT MANGEMENT

Definition

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Restricted Areas

- Orlando Police Department Records, Identification and Traffic Citation Units is a restricted area with unlimited access permitted only to authorized personnel. All other employees, including non-Department al

visitors to the section, will be escorted by an employee with access authorization. These restrictions also apply to the Records storage area in addition to the master fingerprint file room. The Records Unit will ensure that files and computer monitors will not be visible to unauthorized persons.

Hiring /Terminations

- New employee personnel will gain access to all systems upon start date but will lose access to CJI systems if training courses are not completed/ or passed within 30 days. All user accounts of retired, terminated or otherwise former and non-working employees shall be disabled and revoked immediately or as soon as practical. User accounts suspected of compromise shall be immediately disabled upon first discovery of compromise. Logs of access privilege changes shall be maintained for a minimum of one year and the validation process documented. The access level granted to the user for all information systems will be granted based on the satisfactory completion of all personnel security criteria and valid need-to-know/need-to-share as required by assignment of official duties.

- During the employee sign-in process, the Identification Unit personnel shall take fingerprints to be retained in the FDLE Falcon Database, issue a building access card, and prepare an ID badge for the new employee. A copy of the employee's photograph will be forwarded to the Internal Affairs Section and a copy will be filed in the Identification Unit.

- OPD Managers will submit an email to the IT Help Desk Requests for access to computers and software programs and hardware. Requisitions will be submitted to The Quartermaster Unit for uniforms and badges

Termination Process

- A program manager/designee shall complete the top portion of the Orlando Police Department Sign Out Form, which includes the employee's name, identification number, present date, and employment dates. A manager/designee shall instruct the employee to complete the applicable checkout procedures listed on the Orlando Police Department Sign-Out Form. If the employee is not available to complete the sign out form, the program manager/designee is responsible for having the sign-out form completed and submitting the close out form on the employee's behalf. This process includes surrendering the building access card, removal of employees retained fingerprints and an endorsement by Identification Section employee. A Professional Standards Section employee will send an email to Department managers to disable access to various public safety related systems including (ELVIS, Finder, NexTest, OSCO Tiburon) and endorse the Sign Out form.

Annual Review

- All CJI systems (CAD, FINDER, ELVIS FALCON, NEXTEST and CJIS ONLINE etc.) require an annual user audit certifying that users are currently employed by the Orlando Police Department. The assigned system administrator will be responsible to ensure in-active employees are deleted from applications. Once the review is complete, print an active users list and sign the document for future for review during the CJIS Tri-annual audit.

SYSTEM ACCESS CONTROL FOR MULTIPLE CONCURRENT SESSIONS

Definition

Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.

Utilization

- The City of Orlando take steps to ensure that all applications in use at the City of Orlando adhere to secure processes. This includes the authentication of users to prior to granting access to an application and to ensure appropriate access to prevent the modification of hardware or software. The agency implements controls to prevent concurrent client sign on when the application can support the feature.

REMOTE ACCESS

Definition

Remote access is any temporary access to the Agency's information system by a user communicating through an external, non-agency-controlled network (the internet).

The purpose of this policy is to outline acceptable methods of remote access and the security in place to keep the information system(s) secure.

Utilization

- Remote access shall only be used for official use only. This includes those on duty patrol officers remoting in to agency's network using a VPN tunnel**.** Users may not utilize personally owned devices to access the agency's information system at any time. The agency controls all methods of remote access by only allowing agency approved devices connection through the agency VPN. All access is monitored by the information technology Department and reviewed to ensure proper security protocols are being met. If a user is removed from the agency, the user's access to the information system will be terminated immediately to ensure that remote access is denied.

Access

- To access the agency network via a remote connection the agency employee shall make the request, via their immediate supervisor. The IT Security Manager will review the request and reasons for remote access.

VPN

- Remote access using VPN will be allowed through agency owned devices only. No remote access from personally owned devices will be allowed. OPD employees shall be required to sign the remote user agreement prior to a remote access account being established.

Virtual Escorting

- Vendor companies may be granted access to the agency's network only if they are virtually escorted by authorized Agency personnel always. IT will verify the vendor personnel gaining access prior to allowing the session. This will be done through advanced authentication (PIN).

PERSONALLY, OWNED INFORMATION SYSTEMS

Definition

- Personally, owned devices include cell phones, tablets or any other device that is owned and maintained by the user, not the Agency.

Access

- 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.

BYOD

- Bring your own device (BYOD) devices are not authorized.

IDENTIFICATION AND AUTHENTICATION

Definition

OPD's Limited Access Security Officer (LASO) will ensure each person who is authorized to store, process, and/or transmit CJI, as well as those individuals who administer and maintain system(s) that access CJI or the CJIS network is uniquely identified by providing the individual with a unique username and password for access to the information system. The creation of the username and password will occur prior to the individual being granted access.

Password Standards

a. Passwords will be known only to the assigned person and will not be shared.
b. Passwords should be memorized.
c. Passwords will not be stored in data files, printed on reports, taped to work stations, or under keyboards, or programmed on function keys.
d. A password will be created or changed with a minimum of eight (8) characters. The password will consist of upper and lower case alpha characters and numeric characters, no part of the user's name will be used in the password. The password should not be a dictionary word or proper name.
e. Passwords should be sufficiently difficult to prevent unauthorized users from guessing the correct password. The names of children, pets, spouses, favorite teams, favorite bands, telephone number(s), anniversary dates, birth dates, etc. should not be used.
f. Passwords and Usernames will not be the same.
g. Passwords will be changed periodically or immediately if a security breach should arise. Passwords will be changed when a supervisor requests, in writing, the removal of a subordinate's password.
h. Compromised passwords will be changed immediately by contacting the IMS Service Desk.
i. IMS shall implement password complexity to confirm CJIS password requirements are met.
j. Passwords will be set to expire within a maximum of 90 calendar days.
k. Passwords will not be identical to any of the previous 10 passwords.
l. Passwords will not be transmitted in the clear (e.g. using unencrypted communications through http instead of encrypted communications through https) outside of a designated secure location.
m. Systems will be configured to confirm passwords are not displayed when entered.

AUTHENTICATOR MANAGEMENT

Definition

Advanced authenticators are given to users prior to gaining access to criminal justice information outside of the physically secure location. OPD and City IT utilizes Biometrics and Prox Card for Advanced Authentication. The LASO will set up individual user access to retrieve the Biometrics and Prox Card

Assignment

- Authenticators will be assigned to personnel during training or upon reassignment. Any lost, compromised, or damaged authenticators should be reported to the IT Department immediately. Authenticators shall be deactivated immediately if personnel is terminated, retired, or has been reassigned. Each user that accesses criminal justice information must be uniquely identified prior to being given access to the system and information. The Agency uses standard authenticators (passwords) as well as advanced authenticators for accessing criminal justice information in a secure manner.

Rapid Identity application.

- The multi-factor application provides various authentication methods. The application is installed either via manual intervention or via software push from SCCM from a desktop support personnel once a device has been selected and staged for deployment. The key requirement for its use and need is linked to an individual's necessity to access trusted resources. Currently, it is added to all devices used by Orlando PD staff (laptops and desktops alike). Depending on the hardware architecture end users may also require external authentication devices for biometric or RFID proximity reads (this applies mainly for desktops users).

Lost/Stolen/Compromised

- If any of the circumstances above, do come true then the users are encouraged to put in a police report while also calling in the helpdesk line to enter a ticket for tracking purposes. Once the ticket is retrieved by the MFA group will proceed to remove or deactivate the user's profile from within the Rapid Identity's application.

Revocation/Termination

- A Department interface tracks departure. When the task is issued the IT MFA team deletes the account which is different from momentarily deactivating it.

MEDIA PROTECTION

Media in all forms shall be protected always.

Media Storage and Access

- Digital and physical media is restricted to authorized individuals. Only those users of the Agency who have undergone a fingerprint-based record check and have appropriate security awareness training will be allowed to handle criminal justice information in any form.

- All media will be stored in a secure location. Computer equipment will be stored in the secure server room behind locked doors that are only accessible via badge access. Any computer that accesses criminal justice information within the facility will have a screen cover to ensure that information is not viewable by any unauthorized individual. All mobile devices located outside the physically secure location will be in the possession of the individual assigned to the device. When the device is not in use, agency personnel will ensure that the mobile device is locked, and the lid closed.

Physical Records

- Records with CJIS information, must be stored within the Records Section which is only accessed by Records and Identification staff. Any information that must be removed from the records room will be checked out and signed for on the Secondary Dissemination log. Any paper files located with agency officials must stay in the physical control of the agency personnel and locked within filing cabinets when not in use. At no time will the physical media be released to an unauthorized person or left without proper documentation.

Media Transport

- Electronic information that leaves the secure location will be encrypted prior to transmission. To access the information outside of the secure location can only be done by agency personnel utilizing a virtual private network provided by the agency.

- Physical papers that leave the secure location will be stored in a suitcase to ensure that the information obtained within the document cannot be seen by unauthorized individuals. The physical documents will stay with the authorized individuals until there is no further need for the documents. Once the documents have met their purpose, the authorized individual will dispose of the documents In a Blue Bin identified for shredding.

Sanitization and Disposal

- Electronic media that has reached the end of its lifecycle must be sanitized and disposed of to ensure that criminal justice information is not viewed or accessed by unauthorized individuals. Electronic media is

defined as any electronic storage device that is used to record information, including, but not limited to: hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as USB drives.

Hard Drives:

- The Agency overwrites the hard drive utilizing a three-pass wipe. This ensures that the data on the drive is overwritten with patterns of binary ones and zeros. The sanitization of the hard drive is not complete until the third wipe passes, and a verification pass is complete. Destruction of the hard drive will incorporate drilling into the drive. This will be witnessed by authorized Agency personnel.

Disposal

- The agency has an agreement in place with a private vendor that comes onsite to handle the disposal. The CJI is placed in shredding bins until the vendor comes on-site and cross-cut shreds the documents. The process is witnessed by Agency personnel.

PHYSICAL PROTECTION

Definition

The purpose of the physical protection policy is to ensure that CJI and information system hardware, software, and media are physically protected through access control measures.

Security Perimeter

- All electronically-secured doors must be opened with an issued access control card. To move throughout the building and community police offices, plainclothes employees shall display their access card with attached picture identification on the outermost piece of clothing. Uniformed employees shall carry and use their access card to move throughout the building and community police offices. Employees shall ensure that unauthorized persons do not follow any employee through a secured door. All employees remain responsible for the security of their assigned work areas and for locking doors to those areas as may be necessary. When an employee has a name change, the ID unit must be notified within seven calendar days; a new access card must be issued.

Access Cards

- All electronically-secured doors must be opened with an issued access control card. To move throughout the building and community police offices, plainclothes employees shall display their access card with attached picture identification on the outermost piece of clothing. Uniformed employees shall carry and use their access card to move throughout the building and community police offices. Employees shall ensure that unauthorized persons do not follow any employee through a secured door. All employees remain responsible for the security of their assigned work areas and for locking doors to those areas as may be necessary. When an employee has a name change, the ID unit must be notified within seven calendar days; a new access card must be issued.

Visitor Control

- Doors marked Restricted Access do not allow public unescorted access. Visitors must be escorted by an CJIS certified employee

ENCRYPTION

Definition

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates

PUBLIC KEY INFRASTRUCTURE (PKI) is part of proving the requirement used to satisfy dual authentication requirements.

Utilization

The City uses digital certificates as a part of the Advanced Authentication (AA) required for FDLE compliance.

The user-based certificates are used for authentication purposes, and are:

1. Specific to an individual user and not to a particular device.

2. Prohibit multiple users from utilizing the same certificate.

3. Require the user to “activate” that certificate for each use in some manner.

VOICE OVER INTERNET PROTOCOL (VOIP)

Definition

The purpose of this policy is to define standards and procedures for the implementation of Voice Over IP (VoIP) telephone systems as well as lay out restrictions regarding criminal justice information.

Utilization

The agency uses VoIP for the desktop telephone environment. The desktop PC is plugged into the telephone to get connected to the network. The phone has two separate VLANS one for voice and one for data. Even though the PC gets connectivity via the data VLAN on the phone there is no access to the AA data.

Secure Environment

- OPD and IT will:
    - ensure that the underlying data network is configured to host efficient bandwidth and reliability. The VoIP environment will be dedicated only for applications required for VoIP operations.
    - ensure that software patches for the VoIP system and servers originate from the system manufacturer and are applied in accordance with the manufacturer's instructions prior to implementing the patches.
    - ensure that all critical VoIP network and server components are in the physically secured area and that only authorized personnel have access to them.
    - ensure that the default administrative password on the IP phones and VoIP switches are changed prior to implementation.

The data and voice connections on the phone must be segmented by network VLANS to separate the traffic on the VOIP phones.

Patch Management

- Scheduled monthly patch management will occur to mitigate vulnerabilities on computer systems and electronic devices. Change Management entries will be created, reviewed and approved before and after patching occurs.

Restrictions:

1. Do not use mobile software apps to attach to VOIP System.
2. Turn off all unused features on the VOIP System.
3. VOIP phone should not be used for international use (outside the United States and its' territories).

4. Do not store or save criminal justice information on VOIP System.
5. Whenever possible, phones are connected to uninterrupted power sources to prevent an interruption in service due to a power outage.
6. Fax machine are not connected into VOIP System to fax criminal justice information.
7. Alarm systems are not to be connected into VoIP System. Alarm Systems must be connected to copper POTS line.
8. Do not divulge personal or criminal justice information to people you don't know.
9. Be cognizant of discussing criminal justice information using your VOIP Phone on Speaker with unauthorized personnel in the room.
10. Do not install or connect devices to your VOIP Phone such as computers, Bluetooth, recording device, etc.
11. If your VOIP Phone System does not provide a dial tone or is not showing the correct time/date and extension. Employees must call the IT Help Desk for support. The IT may determine if it is a malicious code (i.e., worms, viruses, Trojans), denial-of-service (DoS), distributed DoS (DDoS), and (though non-malicious) flash crowds event.

SECURITY ALERTS AND ADVISORIES

Definition

The City has multiple advisory contacts that provide notifications of security alerts of a wide range of topics, including product vulnerabilities, malicious exports, vendor product alerts, and security partner notifications.

Utilization

The City works to establish relationships with external sources to provide regular information system security alerts and advisories. These alerts are received and distributed to appropriate personnel within the City. Actions taken on these advisories is documented as a part of the City's process to track changes.

WIRELESS USAGE RESTRICTIONS/LOGS/MOBILE DEVICES

Definition

This policy area describes considerations and requirements for mobile devices including

smartphones and tablets. This policy area describes considerations and requirements for mobile devices including smartphones and tablets and the logging

Utilization

The City of Orlando has established restrictions on the use of mobile devices and what they can be used for.

Access

There is no access to the City's internal network from mobile devices such as phones or tablets using any form of communication protocols, such as Wi-Fi, Bluetooth or cellular capability. The City's WI-FI access points do not provide access to CJI controlled data.

Access to the City's internal Wi-Fi network with controlled using Wi-Fi Protected Access cryptographic algorithms.

Physical and administrative access to the management of the Wi-Fi environment is maintained with strong security processes including physical security and strong password security processes.

Logs

Logs from the access point controllers are captured with the City's SIEM log capture solution and stored for at least one year.

BLUETOOTH

Definition

Bluetooth technology is utilized as the open standard for short-range radio frequency communication. This policy provides the minimum baseline standard for connecting Bluetooth enabled devices to the Agency owned devices. The Agency utilizes Bluetooth technologies for operational processes only.

Authorization

- Agency personnel are not authorized to use Bluetooth Technology to access CJIS protected resources.

PERSONNEL SANCTIONS

Violations of this policy will be treated like other allegations of wrongdoing at Orlando Police Department. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but not limited to, one or more of the following:

1. Disciplinary action according to applicable City of Orlando Information Technology policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.