Cocoa Beach Police Department
Standard Operating Procedure

Effective Date: February 24, 2023	**Replaces:** **Amends:** March 15, 2018	**Number:** 305.00
Subject: Information Services Security		**Re-evaluation Date:**
Distribution: ALL PERSONNEL	**Related Standards:** (5th Edition) 26.04M, 32.01M	

This order consists of the following numbered sections:

1. Purpose
2. Scope
3. Policy
4. Definitions
5. User Agreement
6. Certification Requirements
7. Incidence Response
8. Auditing and Accountability
9. Access Control
10. Identification and Authentication
11. Media and Physical Protection
12. Systems, Communications Protections and Information Integrity
13. Personnel Security
14. Mobile Devices
15. FCIC/NCIC Entry, Modify, Locate, Clear, Cancel, BOLO's and Validations
16. Email
17. Data Storage
18. Faxing
19. Logging and Dissemination of CJI
20. Appendices
21. References

1. **PURPOSE**
   To provide guidance to the members of the Department pertaining to usage of department computers, including all computer software, hardware, and other devices issued or installed; email usage, and internet usage.
2. **SCOPE**
   This policy applies to all members of the Department and third party vendors who provide support or services to the Department.
3. **POLICY**
   This document will serve as the Department's local security policy to facilitate implementation of the CJIS Security Policy. It is the policy of the Department to protect the integrity of all information systems such as but not inclusive of: Florida Crime Information Center (FCIC), Criminal Justice Network (CJNet), Drivers and Vehicle Information Database (DAVID), Florida Integrated Network for Data Exchange and Retrieval (FINDER), by protecting the information from unauthorized disclosure, alteration or misuse.
4. **DEFINITIONS**
   A. CRIMINAL HISTORY RECORD INFORMATION (CHRI) - A subset of Criminal Justice Information Services. 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 (CJIS Security Policy 5.5 06/01/2016).
   B. CRIMINAL JUSTICE INFORMATION (CJI) - Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission

and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the Federal Bureau of Investigations Criminal Justice Information Services provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or Personal Information Identifier (PII).

C. CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) - Programs within both the Florida Department of Law Enforcement and the Federal Bureau of Investigation is 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.

D. CRIMINAL JUSTICE NETWORK (CJNET) - A secure, private, statewide intranet system managed and maintained by the Florida Department of Law Enforcement 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.

E. 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.

F. FLORIDA DEPARTMENT OF LAW ENFORCEMENT (FDLE) -The agency responsible for providing the Florida Crime Information Center (FCIC), National Crime Information Center (NCIC), Interstate Identification Index (III), the International Justice and Public Safety Network (Nlets) and Computerized Criminal History (CCH) services to Florida agencies as well as enforcing all policies and regulations mandated by The Federal Bureau of Investigations. FDLE is also responsible for operating and maintaining FCIC.

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

H. INTERSTATE IDENTIFICATION INDEX (III) -The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

I. LAPTOP DEVICES – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OS X, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited feature operating system (e.g. tablets).

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

K. LOCAL AGENCY SECURITY OFFICER (LASO) - The primary Information Security contact between a local law enforcement agency and FDLE under which this agency interfaces with the FBI CJIS Division. LASO 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, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps FDLE informed as to any Information Security needs and problems. The LASO ensures compliance with the FBI-CJIS Security Policy and any other applicable security requirements. The LASO shall be an employee of The City of Cocoa Beach, and is designated by the Chief of Police or designee.

L. 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.

M. 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 which 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. PII shall be extracted from CJI for the purpose of official purposes only. PII must not be electronically disseminated to other agencies.

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

O. Electronic License and Vehicle Information System (ELVIS) – A remotely hosted computer application for accessing FCIC/NCIC, and DHSMV records.

P. Emergency Contact Information (ECI) – Information contained in a motor vehicle record listing individuals to be contacted in the event of an emergency. Emergency Contact Information may be released to law enforcement agencies for purposes of contacting those listed in the event of an emergency.

Q. Personal Communication Device – All cell phones, pagers, personal e-mail devices, personal digital assistants, smart phones, "tablet" style computers and other similar devices.

R. User Account – An account established for agency personnel authorized to use email. Authorized agency personnel shall have a username and password for accessing their account.

S. Software – A computer program; a set of instructions written in a specific language for the computer to perform various operations on data contained in the program or supplied by the user. Software includes, but is not limited to disks, CDs, and screen savers.

5. **USER AGREEMENT**

A. The User Agreements, Management Control Agreements, Security Addendum Agreements, and Private Contractor Agreements between the Department and information system providers are legally-binding documents that cover liability issues and outlines what is expected of each regarding proper use of their systems from that day forward.

B. Whenever the agency head changes, the TAC shall prepare and submit an updated User Agreement to FDLE.

6. **CERTIFICATION REQUIREMENTS**

A. Personnel who have written, computerized or audible access to CJI data will require either Full or Limited CJIS certification or CJIS Online Security certification within six months of initial assignment, and biennially (every two years) thereafter. All personnel, technical support personnel, volunteers and vendors who have physical or logical unescorted access to Department's computer networks with the ability to query or view FCIC/NCIC transactions must maintain CJIS certification at all times. (CFA 32.01D)

B. The TAC shall send email notifications of upcoming expirations to the individuals and their supervisors. All users requiring certification shall contact the agency TAC to arrange for the proper training.

C. If a user lets their certification lapse, regardless of assignment, they shall not access or view CJIS data, nor contact 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.

D. Users who allow their certification to remain expired for two years or more will be required to attend the online instruction. Upon completion users can print a certificate and will understand how to properly handle CJIS-related information.

E. Volunteers, vendors or contract services employees who work in or visit areas where CJI is accessible must complete CJIS Online Security Certification and maintain security certification. This group of individuals does not have the capability to query FCIC/NCIC transactions.

7. **INCIDENT RESPONSE**

A. Upon the detection of any threat or perceived threat on any city owned device, the user is required to immediately disconnect the device from all networks and notify their supervisor promptly.

1. Threat or perceived threats such as but not inclusive of:
    a. Malware
    b. Unauthorized software installation
    c. Unauthorized access
    d. Any other suspicious activity

B. The supervisor shall notify the LASO, providing details of the suspected security incident, using the Security Incident Reporting form as a guide.

C. Once notification has been made the supervisor shall forward the Security Incident Reporting Form to the LASO.

D. The LASO, and/or his designee will investigate the suspected security incident in accordance with The National Institute of Standards and Technology Special Publication 800-61 Revision 2 Titled Computer Security Incident Handling Checklist.
E. The LASO or his designee shall notify the TAC, Deputy Chief and Chief of Police, and if necessary, FDLE using the Security Incident Reporting Form.
F. If a Security Incident Reporting Form is submitted, the form shall be provided to the TAC and retained until the next FDLE audit cycle or until legal action is completed (if warranted).
G. If the incident report is submitted to FDLE, the agency will conduct a lessons learned review and findings may be incorporated into future revisions of the incident handling procedure.
H. Mobile device connectivity to CJI is prohibited. However, if a security incident (loss, theft, or mobile device compromise) occurs involving a city issued mobile device, the following shall be completed.
    1. The user will notify their supervisor immediately and local law enforcement agency if lost or stolen
    2. The supervisor shall notify the LASO, providing details of the suspected security incident, using the Security Incident Reporting form as a guide.
    3. Once notification has been made the supervisor shall forward the Security Incident Reporting Form to the LASO.
    4. The LASO, and/or his designee will investigate the suspected security incident in accordance with The National Institute of Standards and Technology Special Publication 800-61 Revision 2 Titled Computer Security Incident Handling Checklist.
    5. The LASO or his designee shall notify the TAC, Deputy Chief and Chief of Police.
    6. The LASO or his designee will utilize the mobile device management tools (MDM) to perform administrative actions to include locating or remote wipe of the mobile device.

8. **AUDITING AND ACCOUNTABILITY**

A. A security system to safeguard against unauthorized attempts to access, alter, remove, disclose or destroy stored information has been established through a system of assigned authorization levels and passwords. As a security measure and at the direction of IT, personnel will be notified periodically to change computer passwords. (CFA 26.04MA)
    1. When user has 5 consecutive failed log on attempts, the system shall automatically lock the account for 10 minutes unless released by an IT administrator.
B. When a new member requires access to the department's computer system and has been granted authority to the system by the Chief of Police, or his designee, the member shall be added to the system with a user name, password and correct authority level. (CFA 32.01MD)
C. All requests for access to the department's computer system and/or any network server must go through the IT department.
D. When a Department Director or supervisor becomes aware of separation of a member, they will notify the Information Technology Department and Human Resources immediately by sending notifications to the following email addresses: helpdesk@cityofcocoabeach.com and personnel@cityofcocoabeach.com. Information Technology Department designee will remove access to the network within one (1) business day of the separation date. (CFA 26.04MC)
E. The Information Technology Department designee will annually audit the computer system for verification of all passwords, access codes, or access violations.
F. The Cocoa Beach Police Department regulates the use of the Electronic License and Vehicle Information System (ELVIS). This system shall only be used to obtain information for legitimate law enforcement purposes. Information obtained through the system shall not be shared or released to unauthorized persons. Only personnel who have been granted access, received applicable training, or are in a training status under the guidance of a trainer, may access the above system. The entering and retrieval of information shall be in accordance with the rules and procedures established by ELVIS. Requests to query any agency personnel or candidates for employment shall be coordinated by the Human Resources and/or Recruiting Units. Any suspicious activity regarding an agency employee shall be forwarded to the Point of Contact (POC) immediately and the Major or Designee.
    1. ELVIS audits will be conducted as required by the MOU and website audit guidelines, and reviewed by the agency POC. If any questionable use of ELVIS is identified, the Division Commander of the involved employee will be notified. A determination will then be made if an investigation is warranted. The Chief of Police or designee can request additional audits as needed.
    2. Suspected misuse of the ELVIS system shall be investigated pursuant to the procedures outlined in this policy.

9. **ACCESS CONTROL**

A. Restricted computerized records systems (FCIC/NCIC, DAVID, FINDER, LexisNexis, CAD, RMS, etc.) are to be used only to conduct official Department business. Employees are prohibited from using any restricted system for personal or private reasons. Employees are subject to discipline up to and including termination and subject to possible criminal charges for misuse. (CFA 32.01ME)

B. Users will adhere to all of the rules and regulations established by the FBI, the Florida Department of Law Enforcement (FDLE) and the Florida Department of Highway Safety and Motor Vehicles (DHSMV) regarding access to FCIC/NCIC and Drivers and Vehicle Information Databases (DAVID) and maintain the highest level of security possible in light of the environment in which our employees work.

C. Access to CJNet (including FCIC/NCIC), FINDER and DAVID is restricted to the administration of criminal justice only and shall be used for authorized purposes in compliance with FBI/FDLE/DHSMV regulations and operating procedures, and state and federal law. (CFA 32.01ME)

D. A fingerprint based criminal background check and the completion of CJIS Online Security Awareness, Limited Access or Full Access Training (as appropriate to the employee's position) is required before an employee will be authorized to have access to FCIC/NCIC, CJNET, DAVID and FINDER. This includes Information Technology, Public Works, and Fire Department employees with who, in the course of their assigned criminal justice duties, have access to of work on a system or network component that has direct access to FCIC/NCIC, CJNET, DAVID or FINDER.

E. The Department has signed a Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) for access to the Driver and Vehicle Information Database (DAVID).
   1. Information obtained from DAVID can only be disclosed to persons to whom disclosure is authorized under Florida law (FS 119.0712(2)) and federal law (Driver's Privacy Protection Act, 18 USC s. 2721-2725).
   2. Unauthorized disclosure is not only a violation of this policy, but may also subject the violator to criminal and civil penalties.
   3. Emergency Contact Information (ECI)
      a. Emergency contact information contained in a motor vehicle record is confidential and exempt from inspection and copying of records. Without the express consent of the person to whom such emergency contact information applies, the emergency contact information contained in a motor vehicle record may be released only to law enforcement agencies for purposes of contacting those listed in the event of an emergency (refer to FS 119.0712).
      b. Employees are reminded that accessing any DAVID records other than for a law enforcement purpose is prohibited.
      c. Should any supervisor become aware that a subordinate has misused personal information obtained from the DAVID system, he or she shall make immediate notification to the DAVID agency point of contact.
      d. The agency point of contact for DAVID is responsible for notifying the DHSMV of the violation and following their instructions regarding notification to the individual whose personal information has been compromised.
      e. The notification to DHSMV must include the date, number of records affected, and information regarding the notification of the affected individual, the corrective actions and date of actions completed.
   4. Per DHSMV, DAVID photos ARE permitted to be used in photo line-ups for law enforcement investigations when all other alternatives have been exhausted.
   5. Use of the DAVID system is subject to monthly random reviews by the Department's point of contact in addition to conducting a quarterly audit.
   6. Because personal data associated with a driver or motor vehicle record is protected under both federal and state law, and because driver license photographs and social security numbers are highly protected, DHSMV strongly recommends that users not copy and paste data from DAVID into other documents or systems.

F. Unless required to satisfy business needs, access to the Department's network is limited to one active session per user.
   1. Examples of authorized business needs:
      a. Communications center employees logging in to multiple workstations to satisfy dispatching needs.
      b. Power users logged into multiple terminals to assist technical staff

G. Remote access shall only be granted to those vendors through a connection that is FIPS 140-2 certified and with proper certification, for operational business needs. All access of this nature is controlled and monitored.

H. Terminals accessing ELVIS are required to be physically placed in secure locations. Terminal operators must be screened and access to the terminal is restricted. Operators must adhere to all provisions of the FDLE User Agreement.

1. Members are required to treat ELVIS information as sensitive and ensure that the information displayed on terminal screens and information printed from terminals is not visible to un-authorized persons.
2. Any person who may come in contact with sensitive information shall follow current CJIS security awareness guidelines.
3. Agency vehicles equipped with mobile data terminals are classified as a Controlled Area while the Communication Center is classified as a Physically Secure Location.

10. **IDENTIFICATION AND AUTHENTICATION**

A. Each person who is authorized access to restricted computerized records systems shall be uniquely identified by their user name and role. (CFA 32.01MD)

B. Passwords will be used to authenticate a users' unique identification

1. Be a minimum length of 8 characters
2. Not be a dictionary word or proper name
3. Not be the same as your user name
4. Expire within a maximum of 90 calendar days
5. Not be identical to the previous 10 passwords
6. Not be transmitted in the clear outside the secure location
7. Not be displayed when entered

C. The Department does not utilize two-factor authentication as all police vehicles are a physically secure location as defined by CJIS policy.

D. The agency does not utilize public key infrastructure technology

11. **MEDIA AND PHYSICAL PROTECTION**

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse.

A. Viewing

1. Access to any area of the Department, outside of the lobby vestibule and unsecured hallways, by non CJIS certified members is prohibited without escort. (CFA 32.01MD)
2. Entrance to any secure area within the Department, Information Technologies and the Fire Department by any non CJIS certified visitor shall be signed in on a visitor log.
3. All computer screens shall be turned away or powered off if a visitor is present.
4. All hardcopy media shall be removed from the view of a visitor.
5. Once there is no longer a criminal justice need for the physical media it shall be filed, sanitized or destroyed.
6. In areas that are NOT marked "Physically Secure Area," advanced authentication such as Netmotion VPN access must be utilized on agency computers in order to be able to access CJIS data. Additionally, data encryption must be enabled on all hard disks and other media.

B. Storage

1. Documents that have not lost their value or are still being kept for investigative purposes must be kept in a manner to prevent unauthorized or unintended access. (CFA 26.04MB)
2. Backup of IBM systems is completed once every business day and all Windows servers are backed up daily. (CFA 26.04MB)
3. Backup tapes shall be stored in a secure box in a secure area

C. Transport

1. In the event CJIS information needed to be removed from a secure area, it shall be placed in a secure location and only in the possession of a CJIS certified member.

A. Physical,non-digital media, such as files and documents may only be transported in a sealed envelope and carried at all times by authorized CJIS certified member.

B. Agency users must document the removal of physical files from the Agency on an inter-agency dissemination log. The documents must be stamped as "restricted" prior to removal.

i. The log shall include, at a minimum:

a. Description of information being transported.

b. Type of "restricted" information (e.g., CHRI, NCIC Files, RMS records) contained on the media.
c. Name(s) of individuals transporting the information.
d. Authorized recipient(s).
e. Dates sent and received.

ii. Ensure CJIS certified member store media marked as "restricted" information in a locked trunk while in route by vehicle.

A. If a trunk is not available in the vehicle, the media shall be hidden from sight.

iii. Prohibit CJIS certified member from leaving media containing "restricted" information in a vehicle overnight.

2. Back-up tapes shall be transported in a secure box.

D. Disposal
1. Hardcopy media
   a. Agency personnel shall ensure that hardcopy media is destroyed by shredding when the record is superseded, obsolete, the administrative value is lost or a case file is closed.
   b. Criminal histories should not be retained in case files; if a history is needed at a later time, a new history should be obtained.
2. Electronic media
   a. Electronic media must be properly erased/sanitized/wiped prior to disposal
   b. Electronic media must be completely overwritten at least six times to prevent unauthorized access to the previously stored data.

12. **SYSTEMS, COMMUNICATIONS PROTECTIONS AND INFORMATION INTEGRITY**

A. Perimeter boundary security – Firewalls protect all interconnections between the Department's network and other network segments in the city. Access control lists limit the traffic on Department firewalls to only those devices, protocols, ports and/or services necessary. Firewalls are configured to "fail close" rather than fail open in the event of a problem. Firewalls must be kept patched to address vulnerabilities announced by the firewall manufacturer. Default passwords must be changed and unused accounts on firewalls must be deleted.

B. Intrusion Detection Systems - The Information Technology Department's firewalls contain software which detects attempts to compromise the Department's network. The Information Technology Department shall monitor inbound and outbound communications for unusual or unauthorized activities and send individual intrusion detection logs to a central logging facility, where correlation and analysis will be accomplished as a system wide intrusion detection effort. These firewalls also have automated tools to support near real-time analysis of events in support of detecting system level attacks. If any unusual or unauthorized activities are detected, the LASO will complete the Incident Response form and notify the ISO.

C. The Information Technology Department is responsible for maintaining the secure architecture of the network system. 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.

D. The Information Technology Department maintains a secure network architecture ensuring that all CJIS information is encrypted in transit over segments of the internal network not exclusively dedicated for Departmental purposes.

E. The LASO shall maintain an up-to-date network diagram for review and audit purposes. Computers connected to the Department's network are required to have adequate virus protection and software must be up to date with all patches approved by the City of Cocoa Beach Information Technology Department.

F. The Information Technology Department will employ tools that will detect and notify appropriate personnel of events specified in CJIS Security Policy

G. The City of Cocoa Beach utilizes Voice over Internet Protocol (VoIP). All VoIP traffic is segmented on a separate VLAN, and not located on the Department system. The Department prohibits dissemination of CJI over the telephone.

H. The LASO receives security alerts from The Department of Homeland Security and US Computer Emergency Readiness Team. The LASO will disseminate alerts and advisories to appropriate personnel as needed. In the event of an alert that affects the Department's network, the LASO will document the alert and actions taken.

I. Software shall not be installed on any Department network computer without permission from the Information Technology Department. (CFA 32.01MC)

13. **PERSONNEL SECURITY**

A. A name and date of birth criminal history check will be performed on any applicant, contractor, or custodial worker whose job duties would include access to CJI.
   1. If a felony conviction of any kind exists, the applicant is immediately disqualified.
   2. If a record of any kind exists or the person appears to be a fugitive, a Criminal Justice Information (CJI) Access Review Request form will be completed and submitted to FDLE for consideration.
   3. A contractor found to have outstanding arrest warrants are automatically disqualified from access to CJI.

B. A national fingerprint based background check will be completed on individuals with access to CJI, to include support personnel, contractors and custodial workers with unescorted access to physically secure areas, within 30 days of assignment.
   1. If a felony conviction of any kind exists, the applicant is immediately disqualified.
   2. If a record of any kind exists or the person appears to be a fugitive, a Criminal Justice Information (CJI) Access Review Request form will be completed and submitted to FDLE for consideration.
   3. A contractor found to have an outstanding arrest warrant is automatically disqualified from access to CJI.

C. If any person with current access to CJI is subsequently arrested, access will be immediately revoked pending a determination for access from FDLE through the submission of a Criminal Justice Information (CJI) Access Review Request.

D. Certified individuals are expected to comply with all policies and procedures relative to all criminal justice information systems, including, but not limited to, FCIC, CJNet, DAVID, NCIC, CCH, III files and all associated databases and applications. Improper use of information obtained from any FCIC/NCIC and/or related applications and devices may be unlawful, violate federal, state and local policies and may result in prosecution. Any Departmental personnel found in violation of this policy or found misusing PII/CJI and/or CJI applications will be subject to discipline up to and including termination and could be subject to criminal charges in accordance with Florida law (FS 817.568). (CFA 32.01MF)

E. To ensure compliance with the FBI CJIS Security Policy and all related rules, regulations, policies and procedures established for ELVIS, and related networks, only documented, authorized personnel shall be granted access to the various criminal justice information systems; all such authorized users, to include contract law enforcement agencies and its authorized personnel, shall be bound by the security requirements as set forth in Section III of the User Agreement with the Florida Department of Law Enforcement (FDLE). Due to the sensitive nature of the data available on hardware devices and software programs and the associated links with other systems, the following guidelines shall be adhered to:
   1. No information shall be obtained for the personal gain of the user or their acquaintance. Any such use shall result in disciplinary action up to and including termination and/or criminal prosecution.
   2. The transfer of confidential information, intelligence files, and other sensitive materials from agency computers or Personal Communications Devices to non-agency computers, Personal Communications Devices or unauthorized persons, whether in electronic or printed format, is strictly prohibited.
   3. Information obtained through computer interfaces to other state or federal systems (e.g. DAVID and ELVIS), by means of access granted pursuant to F.S.S. 943.0525, can only be used for criminal justice purposes and shall only be accessed by authorized users. Users of CJI shall adhere to all policies, procedures and operating instructions contained in the FBI CJIS Security Policy and all related rules, regulations and technical memoranda published by FDLE.

F. Access to ECI within DAVID and ELVIS is dictated by F.S.S. 119.0712(2)(d)(2). and limits access to law enforcement officials in order to locate and contact family members in the event of an emergency involving the provider of the information.
   1. The Florida Legislature has limited the release of ECI "to law enforcement agencies for purposes of contacting those listed in the event of an emergency." The emergency must involve the person who submitted the information to DHSMV.
   2. ECI shall only be accessed with the approval of a Supervisor and shall only be used for the purpose of notifying a person's registered emergency contact in the event of a serious injury, death, or other incapacitation. ECI shall not be released or utilized for any other purpose, including developing leads or for criminal investigative purposes.

G. Any supervisor who becomes aware that a subordinate has misused personal information obtained from the ELVIS system, shall notify the agency POC immediately, and Major, or Designee.

1. The agency POC for ELVIS is responsible for notifying the appropriate network administrator of the violation and following their instructions regarding notification to the individual(s) whose personal information has been compromised.
2. The notification to the appropriate network administrator shall include the date, and number of records affected.
3. ELVIS violations shall also include:
    a. Information regarding the notification of the affected individual,
    b. Corrective actions, and
    c. Date of actions completed.

H. The Cocoa Beach Police Department has an MOU with the Tallahassee Police Department, allowing access to CJI through ELVIS.
1. All data contained within the ELVIS system is sensitive and privileged information and shall be handled accordingly.
2. To maintain the integrity of this information, the records shall be accorded proper management and security, and shall only be accessed and used by authorized personnel in accordance with agency policy, state and federal law.

I. Activity associated with any aspect of the ELVIS system is subject to detailed monitoring and audits to protect against improper or unauthorized use.
1. Unauthorized use includes, but is not limited to, queries not related to a legitimate law enforcement purpose, personal use, and dissemination, sharing, copying or passing of information to unauthorized users and could result in civil proceedings against the Department and/or criminal proceedings against any user or other person involved.
2. Violations or misuse may also subject the user to administrative and/or criminal charges.

J. The agency POC for ELVIS shall maintain a list of current ELVIS users and ensure proper notifications are made when a user has been deactivated in the system.

14. **MOBILE DEVICES**

A. The Department does not allow the use of personally owned devices, or cell phones to access, process, store or transmit CJI. However, Advanced Authentication compensating controls are in place for agency issued smartphones and tablets.

B. Possession of the agency issued smartphone or tablet is an indication it is the authorized user
1. Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
2. Enable remote device locking
3. Enable remote data deletion
4. Enable automatic data wipe after predetermined number of failed authentication attempts
5. Remote device location (GPS) tracking

C. Wireless networks, including cellular and WiFi, are not considered secure and, as such, Cocoa Beach Police Department's MDT's shall utilize the Netmotion VPN to gain access to the secure network through the firewall.

D. Mobile hot spots assigned to the Department may be used, in accordance with CJIS Security Policy, to facilitate access to CJI only when logged into Netmotion VPN.

E. To prevent the introduction of unlicensed software and computer viruses, all City of Cocoa Beach owned, leased and provided computers are configured with security software and/or settings internal to the operating system designed to prevent unauthorized modification or installation of unapproved software. These measures ensure only authorized employees are allowed to perform software installations.

F. Patch Management – The Department shall identify applications, services, and information systems containing software or components affected by recently announced flaws and potential vulnerabilities resulting from those flaws. The Information Technology Department ensures prompt installation of newly released security relevant patches, service packs, and hot fixes. The Information Technology Department will notify all necessary personnel of any identified security vulnerabilities. If a problem has been identified with recently applied security patches, the Information Technology Department will roll back the security patches until the issue has been identified and resolved. The Information Technology Department will notify the FDLE Information Security Officer via the Security Incident Reporting Form.

G. All laptops that access CJI are subject to monitoring for unusual activity or misuse.

H. The Department does not offer Wi-Fi in its facility.

I. The Department prohibits the usage of Bluetooth to access CJI systems and applications.

15. **FCIC/NCIC**

A. Entry
   1. All information available in a report and/or case file should be entered in the electronic record, and record information entered in FCIC and NCIC must be documented and correspond with information in the agency report and/or case file. In short, all information in the report and/or case file should directly reflect all information in the electronic record.
   2. The responding officer requesting entry of an item into FCIC/NCIC must provide Communications with a report including any identifiers needed for entry as well as narrative prior to the item entry, excluding missing persons and stolen vehicles or boats. Missing Persons, stolen vehicles and stolen boats may be entered as soon as minimum criteria is met for entry. Once the officer completes his/her investigation a report including any identifiers needed for entry, as well as narrative, must be provided to the communications center.
   3. Communications Officers are required to enter all of the information available in the report and supplemental documentation, not just the required fields. Therefore, when making an entry, all information available should be entered. If there is information in the report along with supplemental documentation that is critical to identifying the person or property, and there is not a field available for that information, the additional information should be entered into the Miscellaneous Field. Victim information should never be entered in the Miscellaneous Field.
   4. To enter Missing Persons and lost, stolen or recovered property records, the complainant or victim must file a report with the agency that has jurisdictional responsibility over the case.
   5. The Communications Officers shall query all missing persons and lost, stolen or recovered property through FCIC/NCIC prior to entry and it shall be maintained within the case file.
   6. The Communications Officers must read the report thoroughly to determine what information needs to be entered.
   7. Communications Officers may use additional sources to enhance or "pack" the record entry. Packing the record means to add additional verified information to an entry which will increase the likelihood of the record being hit upon during a query. Any additional information found from other sources must be maintained in the case file. See Appendix Packing The Record – Additional Sources For Record Entry
   8. All records entered should be reviewed for accuracy by another Communications Officer or the case officer within a timely manner. This is what is known as the "second party verification" process.

B. Modify- A record or case report shall be modified as soon as a discrepancy is noted.

C. Locate - After the hit confirmation process has been completed, if the entering agency indicates they want the Department to take the person into custody or recover the property, than a Locate must be placed on the record. The Department cannot place a locate on their own entry. A locate cannot be placed on a record if the entering agency has already removed the entry.

D. Clear - After the hit has been confirmed and the Locate has been placed by the recovering agency, it is the responsibility of the on-duty communications personnel to clear the item from FCIC/NCIC.

E. Cancel - To remove invalid or erroneous records. This includes, but is not limited to, records related to reports discovered to be unfounded or false.

F. Administrative messages - These messages are commonly referred to as BOLOs (Be on the Lookout) or teletypes. Any message sent will include authorized agency "signature" at the end of the message:
   Cocoa Beach Police Department
   (321) 868-3251
   Case report number
   Officer's name/ID number
   User's name/ID number

G. Validations
   1. Every month, the entering agency must review the FCIC/NCIC entry and the original and subsequent documentation in the case file to ensure that the entry is accurate, complete, active and supported by the case report file. The victim, complainant or the court must be contacted to determine if the record is still active, this contact needs to be documented in the case file as to how it takes place (e.g. by phone, certified mail, in person, or on-line). Once the process is completed, the entering agency may modify information in the record, if needed, and must include the validator's name. Validation procedure is attached (see Appendix).
   2. If an original case report containing an FCIC/NCIC record is destroyed or placed off-site, the FCIC/NCIC entry must be removed from the system, since all FCIC/NCIC case report records must be available for confirmation 24 hours a day 7 days a week.

16. **EMAIL**

A. Emailing CJI-related material to include PII is prohibited as the City's email system does not currently meet CJI Encryption standards. If email is the only option, employees may email CJI related materials to include PII from CJNET email to CJNET email ONLY.

B. Employees do not have an expectation of privacy in their use of the City's computer and the e-mail they create, store, send and receive. Electronic communications are neither private nor secure. The City has the right to monitor any and all aspects of its computer and electronic communications system. Use of the City's computer and electronic communication system shall constitute consent to such monitoring and waiver of any right of privacy.

17. **DATA STORAGE**

A. Agency personnel may only use approved Agency removable digital media to store Agency data. The user may request a removable digital device from their supervisor if needed.

B. Universal Serial Bus (USB) Devices (Flash/Thumb /External Drives) - CJI data is prohibited from being stored on personal USB devices.

C. 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. CJI data may be printed on devices within the Department's network or to any location with an Originating Agency Identifier (ORI).

D. 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. CJI data is prohibited from being printed on multi-functional devices outside the Department.

E. Cloud CJI - Employees are prohibited from transmitting or storing data on any Cloud solution. Cloud solutions include Google apps (email, Google Docs, Google Sites), iCloud, Facebook, etc., as those solutions do not currently meet CJIS encryption standards.

F. Bring Your Own Device (BYOD) - Access to CJIS data from any personal device is prohibited.

G. Non-Digital media shall be restricted to only Agency Personnel

a. All non-digital media shall be stored securely within the physically secured location. All records will be stored within the records room with access controlled by proximity badges. Non-digital media printed out by users must be stored within the users' desk or locked filing cabinet.

b. When removing non-digital media, the records staff will verify the requestor of the record to ensure that the request is authorized to access the information. Only approved Agency personnel will be provided the media.

18. **Media Marking**

A. Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact discs, and digital versatile discs, Non-digital media includes paper and microfilm.

B. The Information Technology Team, in conjunction with the Agency LASO will ensure the following procedures are conducted by Agency personnel in regards to media marking:

1. Validate that Agency personnel and information System personnel mark paper and other output products appropriately in accordance with Agency protection requirements, the FBI CJIS Security Policy, and 32 Code of Federal Regulations (C.F.R)

2. Direct Information system personnel and user to adhere to the following when marking documents that contain confidential, restricted or sensitive information:

a. Mark documents appropriately in accordance with applicable policies and procedures set forth by the Agency to that it is immediately apparent that the information shall be protected from unauthorized disclosure.

b. Apply applicable stamps or marks that detail the highest level of protected information contained in the document to the top and bottom of the front and back cover, and on the first and last page.

i. If the last page is not blank, then apply the stamp to the blank back cover.

ii. Annotate all other pages with the highest level of categorization contained on each page.

iii. Pages that contain information not requiring protection should be annotate as "unrestricted".

c. If a document appears as though it may contain information other than "unrestricted", treat that document as if it is "restricted" until status can be verified via Agency chain of command.

d. If Agency personnel are providing the documents to an approved outside source, such as another law enforcement agency, the user must log the exchange in the Agency's dissemination log. The user

must confirm the identity of the requestor prior to providing the information. When providing the requestor the documentation, the user must stamp the documents as outlined above.

3. Mark restricted and sensitive information appropriately and clearly
4. Mark digital media and cover sheets with the following:
    a. Any applicable security markings such as "Restricted".
    b. "Unrestricted" information shall be marked as such, prior to dissemination.
    c. Mark media to the most restrictive protection level of the information contained on the media.

19. **FAXING**

Faxing CJI-related material is prohibited without first being authorized by the Department's TAC. Communications Officers shall not routinely transmit via facsimile (FAX) machine any criminal history data obtained from FCIC/NCIC. Histories may be transmitted by facsimile 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. CJI may be faxed to any location with an Originating Agency Identifier.

20. **LOGGING AND DISSEMINATION OF CJI**

A. Logging criminal history requests- Users are required to log all Criminal Histories, including queries, they run and/or information they disseminate in the Criminal History log book. The following information shall be annotated in the log:

1. Date and time of request
2. Name of subject whose history was run
3. SID #, FBI # or Social Security Number of subject
4. Name of employee or person requesting the criminal history
5. employee number of operator making the query
6. Purpose code
7. Case number
8. Additional notes

B. 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 Criminal History log book. 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:

1. Date and time of request
2. Name of subject whose history was run
3. SID # or FBI # of subject
4. Name of employee or person requesting the criminal history
5. Agency to which the information was released
6. Employee number of operator making the query
7. Reason the information was disseminated
8. Purpose code
9. Case number (if applicable)
10. Additional notes

21. **APPENDIX**

Validation Procedure

22. **REFERENCES**

Florida Department of Law Enforcement, CJIS Security Policy
Florida Department of Law Enforcement, Compliance - Sample Policies

Scott Rosenfeld
Chief of Police
City of Cocoa Beach

Date: 02/10/2023