MONROE COUNTY SHERIFF'S OFFICE

General Order

CHAPTER: 052-E		**TITLE:** CJIS Security
EFFECTIVE DATE: August 13, 2014	**NO. PAGES:** 7	**REVIEWED/REVISED:** January 27, 2021
Sheriff of Monroe County		

I. **PURPOSE:** The purpose of this general order is to define policies that are required for compliance with the Criminal Justice Information Services (CJIS) Security Policy as per the Federal Bureau of Investigation (FBI) and Florida Department of Law Enforcement (FDLE).

II. **SCOPE:** This general order applies to all Monroe County Sheriff's Office (MCSO) personnel.

III. **DISCUSSION:** In order to comply with evolving CJIS Security Policy requirements, it is necessary to separately communicate the CJIS Security Policy requirements as they are developed. These additional requirements are intended to be an enhancement to, but not a replacement of, existing policies.

IV. **DEFINITIONS**:

A. **User:** Any person that is authorized to use the MCSO computer systems.

B. **Software:** Any computer program that is used by MCSO or installed on any equipment owned by MCSO.

C. **Hardware:** Any equipment that is considered a computer, is connected to a computer, is used to access a computer or is used to facilitate remote access to any computer, system or software owned by MCSO. This may include equipment not owned by the MCSO such as personally owned devices or equipment owned by someone else.

D. **CJIS Security Policy:** Security policy established by the FBI and/or FDLE and must be followed in exchange for access to criminal justice information.

E. **Personally Identifiable Information (PII):** 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 FBI 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 a Law Enforcement National Data Exchange (N-DEx) case file.

F. **Criminal Justice Information (CJI):** All of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property and case/incident history data.

G. **Secondary Dissemination:** The release of CJI to any other authorized agency no matter the form of exchange.

H. Security Incident: A violation or possible violation of the technical aspects of the CJIS Security Policy that threatens the confidentiality, integrity or availability of Florida Crime Information Center/National Crime Information Center (FCIC/NCIC).

V. PROCEDURE:

A. Personally Identifiable Information (PII): *CJIS Security Policy 4.3*: PII shall be used for official business only. PII shall be governed under Standard Operating Procedure GEN 118.07 and shall be used interchangeably with "Restricted Data" within that and all other active Standard Operating Procedures

B. Information Exchange: *CJIS Security Policy 5.1.1*

1. Prior to releasing Criminal Justice Information (CJI), MCSO personnel must verify the identity of the person receiving the information and validate that they are authorized to receive the information. In general, this means that the receiver of the information must be employed by a criminal justice agency and have an official business purpose for the information.

2. When CJI is released to any other authorized agency or person, a secondary dissemination logbook shall be maintained with the proper notations prior to releasing the information.

3. This policy shall also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice including, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters and national security clearances.

C. Incident Response: *CJIS Security Policy 5.3*.

1. All authorized users are responsible for the protection of information subject to confidentiality concerns in systems, archived, on backup media, and until destroyed.

2. All authorized users are also responsible for assuring threats, vulnerabilities and risks associated with accessing CJIS systems and services are eliminated prior to accessing the CJIS system.

3. Any security incidents that may arise shall be reported immediately to your chain of command for action deemed necessary. The chain of command will immediately report the security incident to the Information Systems (IS) Department.

4. You may see only indicators of a security incident which may include, but are not limited to, the following:

    a. The system unexpectedly crashes without clear reasons

    b. New user accounts are mysteriously created which bypass standard procedures

    c. Sudden high activity on an account that has had little or no activity for months

    d. New files with novel or strange names appear

    e. Accounting discrepancies

    f. Changes in file lengths or modification dates

g. Attempts to write to system files

h. Data modification or deletion

i. Denial of service

j. Unexplained poor system performance

k. Anomalies

l. Suspicious probes

m. Suspicious browsing.

5. The Local Security Officer shall, upon review of the suspected incident, report the incident to the FDLE ISO via email at CJISCSO@fdle.state.fl.us. The message subject line shall say "Possible Security Incident", and the email body shall include the following information: date of the incident, locations of incident, systems affected, method of detection, nature of the incident, description of the incident, actions taken, resolution and contact information for the agency.

D. Access Control: *CJIS Security Policy 5.5.2.2 (1)*

1. MCSO prohibits running multiple concurrent active sessions on different computers within CJI systems.

2. Some areas may be approved to run multiple concurrent active sessions on the same computer based on job requirements. E.g. dispatch personnel may operate multiple concurrent CAD sessions on the same computer as long as all other policies and procedures are complied with.

E. Wireless Access Restrictions and Wi-Fi Logs: *CJIS Security Policy 5.5.7 and 5.13*

1. Only Wireless Access Points installed, controlled and configured by Information Systems are allowed on the MCSO network.

2. All MCSO wireless network traffic, both cellular and 802.11, shall be monitored, controlled, and restricted to authorized usage only. Automated monitoring systems will be setup, configured and maintained to monitor all aspects of the network (wired and wireless) for unusual activity. The automated monitoring systems will alert the IS Department staff to any suspected issues or concerns. Wi-Fi logs shall be reviewed on a regular basis.

F. Authentication Strategy: *CJIS Security Policy 5.6.2*

1. All MCSO users will comply with the general orders in regards to the access to and use of MCSO computer hardware, software, network and technology systems.

2. Additionally, all MCSO in-car mobile computer users shall use advanced authentication security measures as deployed by the IS Department. The advanced authentication system will be compliant with the CJIS Security Policy requirements. Examples may include hardware tokens, software tokens, certificates and other approved measures.

G. Physical Protection: *CJIS Security Policy 5.9:* All hardware and software that processes, stores or transfers CJI shall be physically protected through access control measures to include, but not limited to, physical barriers, physical locks, electronic locks controlled by badge readers or direct supervision by MCSO personnel.

H. Actions in Response to Alerts: *CJIS Security Policy 5.10.4.4*

1. MCSO personnel shall, for their area of responsibility, receive, disseminate, document and react to validated security alerts and bulletins in compliance with general orders and the CJIS Security Policy. Any relevant alerts shall be forwarded to Information Systems by the appropriate supervisor.

2. Based upon the information contained in the alerts or bulletins, the information will be disseminated to appropriate MCSO personnel.

3. Based upon the information contained in the alerts or bulletins, appropriate actions will be taken by IS Department staff

I. Patch Management: *CJIS Security Policy 5.10.4.1*

1. The IS Department identifies and enforces patch management for all critical and security related patches. All CJIS facing systems are patched at least monthly to include:

   a. Testing of appropriate patches before installation. Rollback capabilities when installing patches, updates, etc.

   b. Automatic updates without individual user intervention.

   c. Centralized patch management.

2. Patch requirements discovered during security assessments, continuous monitoring or indicated response activity shall be addressed expeditiously. The IS Department shall employ virus protection mechanisms to detect and eradicate malicious code at critical points throughout the network. The IS Department shall ensure malicious code protection is enabled at all critical points.

J. Remote Access: *CJIS Security Policy 5.5.6*: Remote access shall be used for official use only. This includes deputies remoting in to the agency's network using a VPN tunnel. IS personnel may remote access into the agency's network only for emergency purposes. Vendor companies may be granted access to the agency's network only if they are virtually escorted by authorized personnel at all times.

K. Personally Owned Information Systems: *CJIS Security Policy 5.5.6.1*: Personally owned devises are not allowed to access the agency's network. Therefore, a device that is not owned by the Monroe County Sheriff's Office shall not process, store, access or transmit CJI.

L. Authenticator Management: *CJIS Security Policy 5.6.3.2(2)*: Authenticators will be assigned to personnel during training or upon reassignment. Any lost, compromised or damaged authenticators should be reported to the IS department immediately. Authenticators shall be deactivated immediately if a person is terminated, retired or has been reassigned.

M. Bluetooth: *CJIS Security Policy 5.13.1.3*: Bluetooth will only be used for official business purposes. The purposes include the agency's Rapid IDs, printers and wireless mice. All other Bluetooth devices shall be approved by the MCSO IT department.

N. INFORMATION HANDLING

1. 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 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.

2. The Agency 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 Agency employees. The servers are encrypted with FIPS 140-2 certified encryption in order to secure the criminal justice data stored on them.

3. Physical information, such as reports that contain criminal justice information are stored in the areas and/or rooms that is only accessible to Agency personnel. The documents are stored in a sealed container/room and are only removed when needed for operational purposes. When removed, the information is kept by an authorized individual and then returned.

4. Any information that must leave the facility for transport will be done so only by authorized personnel and only for operational purposes. All computers within the facility are turned away from view to prevent unintentional viewing or shoulder surfing. The agency does not allow CJI to be transmitted externally via email.

O. ACCOUNT MANGEMENT

1. 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.

2. The agency maintains management of all information system accounts to include establishing, activating, modifying, reviewing, disabling, and removing accounts as necessary for each individual. The management of CJI system accounts shall be conducted by Information Technology personnel at the direction of the LASO in accordance with all policies and CJIS Security Policy requirements.

3. 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.

P. MEDIA PROTECTION: Media in all forms shall be protected at all times.

1. **Media Storage and Access**

   a. 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 within secure locations. 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.

b. Physical paper files will be stored within the physically secure location which is only accessed by records staff. Any paper files located with agency officials will 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.

2. **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 folder 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 accordingly.

3. **Digital Media Sanitization and Disposal**

a. 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.

b. All electronic media must be properly sanitized before being transferred from the custody of the Agency. The proper method of sanitization depends on the type of media and the intended disposition of the media.

c. Destruction of the hard drive will incorporate degaussing. This will be carried out or witnessed by authorized Agency personnel.

d. USB drives, floppy disks, rewritable CD-ROMS, zip disks, videotapes and audiotapes will be erased if able and then destroyed, witnessed or carried out by authorized Agency personnel.

4. **Disposal of Physical Media**

a. The disposal of criminal justice information must be done in an effective manner in order to protect the secure information. The purpose of this policy is to lay out the proper disposal and destruction of physical media within the Agency.

b. When no longer needed, physical media such as hard copy print-outs shall be disposed of by shredding using an agency owned cross-cut shredder. The shredding will be done by authorized agency personnel.

4. VOICE OVER INTERNET PROTOCOL (VOIP)

a. Voice over Internet Protocol (VoIP) is the routing of voice conversations over a packet switched network as opposed to the traditional circuit-switched telephone network. Voice and data convergence introduces many security issues that must be addressed prior to deployment and use of VoIP technology. The purpose of this policy is to define standards and procedures for the implementation of VoIP telephone systems as well as lay out restrictions in regards to criminal justice information.

b. Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

c. Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

d. To ensure the secure environment of the VoIP system, the Agency will enable the underlying data network is configured to host efficient bandwidth and reliability. The VoIP server will be dedicated only for applications required for VoIP operations.

e. IT will 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.

5. **ENCRYPTION:** Public Key Infrastructure (PKI) Technology: At the moment the agency does not utilize PKI.