MONROE COUNTY SHERIFF'S OFFICE

General Order

CHAPTER: 052 E		**TITLE:** CJIS Security
EFFECTIVE DATE: August 13, 2014	**NO. PAGES:** 4	**REVIEWED/REVISED:** 11-14-17
REFERENCE:		**RESCINDS:**
 **Sheriff of Monroe County**		

PURPOSE: The purpose of this standard operating procedure is to define policies that are required for compliance with the CJIS Security Policy as per the FBI and FDLE.

SCOPE: This Standard Operating Procedure shall apply to all Sheriff's Office personnel.

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 Standard Operating Procedures.

DEFINITIONS:

- **User**- Any person that is authorized to use the Monroe County Sheriff's Office computer systems.
- **Software**- Any computer program that is used by the Sheriff's Office, or installed on any equipment owned by the Sheriff's Office.
- **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 the Sheriff's Office. This may include equipment not owned by the Sheriff's Office such as personally owned devices or equipment owned by someone else.
- **CJIS Security Policy**- Security policy established by the FBI and/or FDLE, and must be followed in exchange for access to criminal justice information.
- **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.

- **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.
- **Secondary Dissemination** - The release of CJI to any other authorized agency no matter the form of exchange.
- **Security Incident** - A violation or possible violation of the technical aspects of the CJIS Security Policy that threatens the confidentiality, integrity, or availability of FCIC/NCIC.

PROCEDURE:

- 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
- Information Exchange - *CJIS Security Policy 5.1.1*
  - Prior to releasing Criminal Justice Information (CJI), Sheriff's Office 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.
  - 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.
  - 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.
- Incident Response - *CJIS Security Policy 5.3*.
  - All authorized users are responsible for the protection of information subject to confidentiality concerns- in systems, archived, on backup media, and until destroyed.
  - 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.
  - 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 Division.
  - You may see only indicators of a security incident, these incidents may include, but are not limited to, the following:
    - The system unexpectedly crashes without clear reasons
    - New user accounts are mysteriously created which bypass standard procedures
    - Sudden high activity on an account that has had little or no activity for months
    - New files with novel or strange names appear

        - Accounting discrepancies
        - Changes in file lengths or modification dates
        - Attempts to write to system files
        - Data modification or deletion
        - Denial of service
        - Unexplained poor system performance
        - Anomalies
        - Suspicious probes
        - Suspicious browsing.
    - 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 I resolution and contact information for the agency.

- Access Control - *CJIS Security Policy 5.5.2.2 (1)*
    - The Sheriff's Office prohibits running multiple concurrent active sessions on different computers within CJI systems.
    - 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.
- Wireless Access Restrictions and Wi-Fi Logs - *CJIS Security Policy 5.5.7 and 5.5.7.1 (13)*
    - Only Wireless Access Points installed, controlled and configured by Information Systems are allowed on the Sheriff's Network.
    - All Sheriff's Office 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 Information Services Division staff to any suspected issues or concerns. Wi-Fi logs shall be reviewed on a regular basis.
- Authentication Strategy - *CJIS Security Policy 5.6.2*
    - All Sheriff's Office users will comply with Sheriff's Office General Orders in regards to the access to and use of Sheriff's Office computer hardware, software, network, and technology systems.
    - Additionally, all Sheriff's Office in-car mobile computer users shall use advanced authentication security measures as deployed by the Information Systems Division. 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.
- 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 Sheriff's Office personnel.
- Actions in Response to Alerts - *CJIS Security Policy 5.10.4.5 (3)*

- Sheriff's Office 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.
- Based upon the information contained in the alerts or bulletins, the information will be disseminated to appropriate Sheriff's Office personnel.
- Based upon the information contained in the alerts or bulletins, appropriate actions will be taken by Information Services Division staff

- Patch Management - *CJIS Security Policy 5.10.4.1*
  - The Information Systems Division identifies and enforces patch management for all critical and security related patches. All CJIS facing systems are patched at least monthly to include:
    - Testing of appropriate patches before installation. Rollback capabilities when installing patches, updates, etc.
    - Automatic updates without individual user intervention.
    - Centralized patch management.
  - Patch requirements discovered during security assessments, continuous monitoring, or indicated response activity shall be addressed expeditiously. The Information Systems Division shall employ virus protection mechanisms to detect and eradicate malicious code at critical points throughout the network. The Information Systems Division shall ensure malicious code protection is enabled at all critical points.
- Remote Access- CJIS Security Policy 5.5.6
  - Remote access shall only be used for official use only. This includes Deputies remoting in to the agency's network using a VPN tunnel. IT 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.

- 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.
- 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 IT department immediately. Authenticators shall be deactivated immediately if personnel is terminated, retired or has been reassigned.
- 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 devises shall be approved by the agency's IT department.