



ADMINISTRATIVE PROCEDURE			1106.01	
<div><div></div><div>CRIMINAL JUSTICE INFORMATION SERVICES SECURITY POLICY</div><div></div></div>				
ISSUED: 10-12-2013	EFFECTIVE: 10-22-2013	REVISED: 10-19-2023	REVIEWED: 10-19-2023	PAGES: 3

CONTENTS

This procedure consists of the following numbered sections:

- I. GENERAL PROCEDURES
- II. AWARENESS AND TRAINING

PURPOSE

This standard operating procedure will establish agency policy and procedure for access and usage of the Florida Department of Law Enforcement (FDLE) Criminal Justice Information Services.

SCOPE

This procedure shall apply to all agency personnel accessing or using information obtained from the Florida Crime Information Center and the National Crime Information Center.

DISCUSSION

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. FDLE Criminal Justice Information Services provide the data. This policy is to address specific security provisions of the FDLE Criminal Justice Information Services Security Policy; Version 5.9.2 dated December, 2022. Punta Gorda Police Department Standard Operating Procedures and City of Punta Gorda Computer Security Incident Response Team Procedures are drafted to comply with FDLE Criminal Justice Information Security Policy.

DEFINITIONS

1. **Personally Identifiable Information (PII):** 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. PII extracted from CJI is for official business only.
2. **Florida Criminal Justice Network:** A limited-access website operated by the Florida Department of Law Enforcement that provides various resources and database access to criminal justice agencies. (<http://www.flcjin.net>).
3. **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.
4. **CJIS Security Policy:** The FBI CJIS Security Policy document as published by the FBI CJIS ISO.
5. **Florida's Integrated Criminal History System (Falcon):** Provides access to the criminal justice community through fingerprint devices and a web interface.

PROCEDURE

I. GENERAL PROCEDURES

- A. **CJI Handling:** Agency personnel accessing and using information obtained from eAgent or the state Driver and Vehicle Information Database (DAVID) will comply with the Criminal Justice Information Services (CJIS) Security Policy and the information safeguards stated in the Memorandum of Understanding (MOU) executed with the Florida Department of Transportation, Division of Highway Safety and Motor Vehicles (DHSMV). Information obtained under the provisions of the MOU will only be disclosed to persons to whom disclosure is authorized under Florida law and federal law. These procedures apply to the exchange of CJI no matter the form of exchange.
- B. **Noncriminal Justice Purpose:** Information collected for noncriminal justice purposes such as employment eligibility, licensing determinations, immigration and naturalization matters and national security clearances shall be disclosed to persons to whom disclosure is authorized under Florida law and federal law.

- C. Multiple Concurrent Sessions: It is the practice of the Punta Gorda Police Department to allow their members to be logged on concurrently to approved department computers to facilitate their duties. Members must take appropriate safeguards to prevent information in a different concurrent session from being compromised.
- D. Security Incident Response: In the event security has been compromised, the Punta Gorda Police Department will submit the Computer Security Incident Response Capability (CSIRC) reporting form to the FBI CJIS CSIRC point of contact, 1000 Custer Hollow Road, Module D-2, Clarksburg, WV 26306-0102.
- E. Users with Security Responsibilities: The User with Security Responsibilities shall be a member of the City of Punta Gorda's Information Technology Division and be designated by the IT Manager.
- F. CJIS Data: The Punta Gorda Police Department members are prohibited from storing CJIS data on any portable storage device unless the device is encrypted to FIPS 140-2 standards.
- G. Department Issued Cell Phones: Department members are prohibited from accessing CJIS data on department issued cell phones. This includes accessing DAVID, accessing any criminal history information or taking evidentiary photos or videos outside of Axon Capture.
- H. Inactivity: If during the quarterly DAVID audit, a member has been identified as being inactive for more than ninety (90) days through DAVID or eAgent, the auditor shall determine if the member shall be disabled. If such member shall not be disabled the auditor shall document as to such determination.
- I. Falcon: Retained Applicant Users are responsible for reviewing their agency's list of retained applicants to determine whether those records should continue to be retained. In addition to employees, an agency's list of retained applicants should contain records for any individuals granted unescorted access to the CJA's CJIS secure areas and/or computer systems.
 - a. Falcon Audits shall be completed once every six months and shall be submitted to Staff Inspections.

II. AWARENESS AND TRAINING: Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. Users with Security Responsibilities require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

- A. Role-based security and privacy training shall be provided to personnel with the following roles and responsibilities:
1. All individuals with unescorted access to a physically secure location;
 2. General user: A user, but not a process, who is authorized to use an information system;
 3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform;
 4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.
- B. System users shall receive Security and Privacy Literacy training.
- C. All Training shall be completed prior to accessing the system, information, or performing assigned duties and annually thereafter or when required by system changes.
- D. CJIS Security Policy section 5.2.3 describes the topics that must be addressed within each Role-Based Security Awareness Training and can be located at <https://www.flcjin.net/Information-Security/Documents/CJIS-Security-Policy.aspx>.

APPROVED



PAMELA R. SMITH, CHIEF OF POLICE

STAFF REVIEW DATES: 11-05-2013, 11-21-2013, 03-30-2016, 03-27-2018, 12-03-2019, 12-03-2021, 10-19-2023

REVISION DATES: 11-05-2013, 11-21-2013, 03-30-2016, 03-27-2018, 08-14-2019, 12-03-2019, 03-27-2020, 08-13-2021, 12-03-2021, 02-07-2023, 09-26-2023, 10-19-2023