



GENERAL OPERATIONS			1106.03	
<div><div></div><div>JAIL RECORDS MANAGEMENT SYSTEM (JMS) AND CRIMINAL JUSTICE INFORMATION EXCHANGE</div><div></div></div>				
ISSUED: 12-18-2020	EFFECTIVE: 01-16-2021	REVISED: 11-19-2023	REVIEWED: 11-19-2023	PAGES: 3

CONTENTS

This procedure consists of the following numbered sections:

- I. RESPONSIBILITIES OF THE PUNTA
GORDA POLICE DEPARTMENT

PURPOSE

This standard operating procedure establishes guidelines for the usage of the Jail Records Management System (JMS) as well as guidelines for the retrieval of Criminal Justice Information (CJI) from the Charlotte County Sheriff's Office.

SCOPE

This procedure shall apply to all Punta Gorda Police Department personnel.

DISCUSSION

A Memorandum of Understanding has been entered between the Charlotte County Sheriff's (CCSO) and the Punta Gorda Police Department (PGPD) establishing a relationship between the parties under which the Charlotte County Sheriff's Office will share Criminal Justice Information and grant limited access to the Charlotte County Jail Records Management System to the City of Punta Gorda.

DEFINITIONS

1. **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.
2. **CJIS Security Policy:** The FBI CJIS Security Policy document as published by the FBI CJIS ISO.

PROCEDURE

I. RESPONSIBILITIES OF THE PUNTA GORDA POLICE DEPARTMENT

- A. In accordance with the Memorandum of Understanding the Punta Gorda Police Department shall:
 1. Abide by all applicable local, state, and federal laws, rules, and regulations with regards to the use of JMS and CJI.
 2. Abide by all the terms and conditions of the Criminal Justice User Agreement executed between FDLE and CCSO, to include but not limited to the [FBI CJIS Security Policy](#).
 3. Make use of the records for authorized criminal justice purposes only.
 4. Disseminate CJI related information obtained from CCSO only for criminal justice purposes.
 5. Notify CCSO via email ([See Policy Appendix XI\(C\)\(1\)](#)) within 24 hours of a member of PGPD ceases employment in order for CCSO to deactivate such member's access to JMS.
 6. Maintain any information obtained from the CCSO in a secure place and destroy records containing such information in compliance with all applicable federal and state laws.
 7. Ensure all CJIS data transmitted over any public network segment be encrypted as required by the FBI CJIS Security Policy.
 8. Ensure all devices with connectivity to the JMS and CJI employ virus protection software and such software shall be maintained in accordance with the software vendor's published updates; and will promptly and fully patch Windows and other software present on all such devices, after any necessary testing, upon such patches becoming available.

9. Agree that JMS and CJI may only be accessed via computers or interface devices owned by PGPD or a contracted entity. Personally owned devices shall not be authorized to access, process, store, or transmit JMS or CJI.
10. Agree that personnel who access JMS and CJI via CCSO for purposes that are not authorized, disclose information to unauthorized individuals or in an unauthorized manner, or violate CJIS rules, regulations, or operating procedures is a violation of department policy and is covered in [Standard Operating Procedure 304.00 – Standards of Conduct](#).
11. Agree the Support Services Division Commander or designee will be the point of contact for the purpose of receiving and disseminating, as appropriate, information concerning unauthorized publication or release of CJI for follow-up and disciplinary action as appropriate. PGPD will conduct appropriate follow-up and will notify CCSO's Point of Contact of the outcome of investigations related to violations of this agreement.
12. Agree to submit instances of misuse of CJI or JMS information obtain by PGPD from CCSO to CCSO. Instances of misuses should be submitted to CCSO via email ([See Policy Appendix Section XI\(C\)](#)) within 48 hours of the completion of PGPD internal investigation. PGPD understands that CCSO has an obligation to report instances of misuse to the FDLE for follow up of applicable investigation and discipline in compliance with the FBI CJIS Security Policy.
13. Agree that CCSO reserves the right to deny CJI or related records or access to JMS to any individual based on valid, articulable concerns for the security and integrity of CJIS and related programs/systems information.

APPROVED

PAMELA R. SMITH, CHIEF OF POLICE**STAFF REVIEW DATES:** 10-19-2023**REVISION DATES:** 10-19-2023