GENERAL OPERATIONS	1206.02

	FLORIDA REGIONAL LAW ENFORCEMENT EXCHANGE (RLEX)	

ISSUED: 05-20-2016	EFFECTIVE: 05-30-2016	REVISED: 10-23-2025	REVIEWED: 10-23-2025	PAGES: 6

CONTENTS

This procedure consists of the following numbered sections:

I. GENERAL
II. N-DEX

III. RLEX
IV. SYSTEM ADMINISTRATION

SCOPE

This procedure shall apply to all agency personnel accessing or using information obtained from the Florida Regional Law Enforcement Exchange (RLEX).

DISCUSSION

The Florida Regional Law Enforcement Exchange (RLEX) is a law enforcement information sharing system that is designed to assist agencies in solving crime and fighting terrorism through improved data sharing. The purpose of the RLEX system is to allow participating agencies to contribute data (principally records management and jail management systems) in a format which will give other participating agencies the ability to query the data.

DEFINITIONS

1. **Florida Regional Law Enforcement Exchange (RLEX):** A law enforcement information sharing system.

2. **Law Enforcement Information Exchange (LInX):** A data sharing initiative as the core mechanism for access to the data.

3. **Florida Regional Law Enforcement Information Exchange (FL-RGNL):** The warehouse of data for participating agencies. FL-RGNL enables RLEX to query other LInX systems beyond the FL-RGNL region of LInX to access other regions across the country and the N-DEx.

4. **FBI National Data Exchange (N-DEx):** Federal Bureau of Investigation data exchange system.

5. **Primary Point of Contact:** Agency member or employee designated by the Chief of Police to manage and supervise the RLEX system at the agency level.

PROCEDURE

I. GENERAL

A. User accounts are authorized to all sworn law enforcement members, members of the Communications Section and members of the Records Section. Volunteers assigned to the Criminal Investigations Section who have completed a full law enforcement background equivalent to that of police officer are also eligible for system access. Additional accounts may be authorized in writing by the Chief of Police.

B. RLEX is not intended by the participating agencies to operate or be used as a criminal history system or a criminal intelligence system governed by the provisions of Title 28, Parts 20 and 23 respectively, of the Code of Federal Regulations.

II. N-DEx

A. Participation: The Punta Gorda Police Department will participate in the FBI's National Data Exchange (N-DEx) system. FDLE CJIS will include N-DEx audits in its normal triennial CJIS audits of each participating agency. All such audits of N-DEx access through RLEX will be "system use" audits to assess the Participating Agencies' understanding of and compliance with N-DEx policies and requirements, as well as those of RLEX. The audits may also review the frequency of submissions of data to N-DEx.

B. Use: Our agency may use N-DEx to conduct criminal justice employment background checks, including the screening of employees or applicants of other agencies over which participating agencies maintain management control, provided the correct use code "J" is selected and the User follows official FBI CJIS policy regarding Notice and Consent, Redress and Use Code J, as explained in the current Criminal Justice Information Services Law Enforcement National Data Exchange (N-DEx) Policy and Operating Manual ("N-DEx Policy Manual"). The Punta Gorda Police Department has modified the User's Notice and Consent form to the applicant for employment as described in Appendix A: N-DEx Criminal Justice Employment Screening Requirements in conjunction with the RLEX Memorandum of Understanding.

III. **RLEX**

A. Use and Dissemination

1. Each Agency retains sole ownership of and sole responsibility for the information it contributes, and may at will at any time update, correct, or delete any of its information contained in RLEX. All system entries will be clearly marked to identify the contributing Agency.

2. Each Agency will be responsible for ensuring sealed or expunged records are updated as such within the RLEX system. The action will occur as an automated process, but can be performed manually by the agency should the automated process fail.

3. The contributing Agency has the sole responsibility and accountability for ensuring that no information entered into RLEX was obtained in violation of any Federal, State, or local law applicable to the contributor and for ensuring compliance with all laws, regulations, policies, and procedures applicable to the Agency's entry and sharing of information into RLEX, to include, but not limited to, firearm ownership data prohibited from being compiled by Section 790.335, Florida Statutes.

4. An RLEX user may print a record from any RLEX agency and retain said copy to assist with case investigation. Destruction of the said copy may only take place in accordance with applicable Florida public record retention requirements. An RLEX user may print a record from any other Regional LInX agency; however the retention time for all other Regional LInX agencies is 72 hours. At the end of the 72-hour period said user must destroy the copy. No records printed from a LInX system, including RLEX, may be used as part of any investigative case file. A user must obtain an official record and approval from the contributing agency, regardless of where the agency is located, in order to use in an investigative case file.

5. Participating Agencies will not release information generated by another Agency without first consulting the originating (contributing) Agency to determine the current status of that information. Information which is exempt from disclosure by law may not be released without the permission of the originating Agency.

6. Information obtained from the RLEX system, including analytical products derived therefrom, shall not be used as a basis for enforcement or other official action, including employment screening or screening of contractors and vendors, unless the user Agency first notifies and verifies the reliability and accuracy of the information with the Agency(s) that contributed the information in question.

7. Immediate dissemination of RLEX information without permission can be made if:

   a. There is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to the national security; or

b. It is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to such a threat, danger, or harm.

8. Information in the system shall not be disseminated outside of an accessing Agency without first obtaining express permission of each Agency that contributed the information in question unless the information is subject to disclosure by court order or applicable law. The owner of the information shall be subsequently notified of any and all disseminations made under this exception.

B. Access

1. Each agency may restrict any investigative information to the extent deemed necessary for confidentiality or security purposes.

2. An Agency member may not access RLEX unless he or she has a legitimate, official need to know for an authorized criminal justice purpose.

   a. Authorized criminal justice purpose includes preliminary screening of applicants (including contractors and vendors) for employment with an Agency; provided that no action in this regard will be taken based solely on information retrieved from the RLEX system, and that such information must be verified and substantiated, independently of its presence in RLEX, before any action is taken.

   b. Any use made of information derived from or related to data in the RLEX system for employment or contractor/vendor screening must be consistent with applicable state and federal law.

3. RLEX information shall not be included in any official case file, nor used in the preparation of judicial process such as search or arrest warrants (with accompanying affidavits) or subpoenas.

4. References to the RLEX database should be avoided in lieu of references to the original source documentation.

C. Training

1. Any Agency member directly accessing the RLEX system must hold a current FDLE CJIS certification or have completed Security Awareness Training as required by the FBI CJIS Security Policy.

IV. **SYSTEM ADMINISTRATION**

A. The Administrative Services Supervisor shall:

1. Serve as the Punta Gorda Police Department's Point of Contact;

2. Have access to that Agency's portion of the users audit log;

3. Maintain the audit log files to avoid unauthorized changes or destruction;

4. Ensure that any agency members directly accessing the RLEX system hold a current FDLE CJIS certification;

5. Exercise supervisory authority over the operation of N-DEx;

6. Train on N-DEx policies;

7. Adhere to authorized use/dissemination of N-DEx information;

8. Attend and participating in the N-DEx audit process;

9. Maintain agency-level records pertaining to N-DEx users and notifying the CSO of any changes;

10. Report violations or incidents of attempts to compromise N-DEx, R-LEX, or information contained within the systems, immediately to RLEX and the CSO;

11. Ensure completion of fingerprint-based criminal history checks on all N-DEx users and notify the CSO if an arrest history is found;

12. Ensure along with the Agency Source Data Administrator (SDA), as described in the N-DEx Policy Manual, that the configurable information sharing controls are set according to Agency requirements;

13. Ensure adherence to the N-DEx Policy Manual, CJIS Security Policy, and this Agreement in their submission, access, and use of N-DEx information;

14. Conduct an annual audit of all Agency users of N-DEx to include confirming that those users are eligible to participate in N-DEx; and notifying the CSO of all users, upon request or as needed to maintain currency and completeness of the list of users.

15. Will designate those employees who have access to RLEX and agrees to use the same degree of care in protecting information accessed as it exercises with respect to its own sensitive information;

16. Add and delete users from the RLEX system;

17. Promptly revoke user access to the RLEX system when the user no longer requires or no longer is permitted access to the RLEX system or has separated from the Agency;

18. Ensure that each user has a current telephone number and email address associated with his or her profile in RLEX; and

19. Report any misuse to the Chief of Police and take appropriate corrective administrative and/or disciplinary action against any of its personnel who misuse the RLEX system, as the agency would if it were an abuse of sensitive information in its own record system.

APPROVED

(signature)

PAMELA R. SMITH, CHIEF OF POLICE

STAFF REVIEW DATES: 05-28-2019, 04-06-2021, 10-19-2023, 10-23-2025

REVISION DATES: 05-25-2019, 04-06-2021, 10-19-2023, 10-23-2025