	ROCKPORT POLICE DEPARTMENT	
	Chapter 5 Information and Records Management	
	Policy 5.4 Automated License Plate Readers	
	Effective Date: 12/18/2023	**Replaces** Previous versions
	Approved: _____ Gregory W. Stevens, Chief of Police	
	Reference: N/A	

I. POLICY

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. ALPRs are used by the RPD to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance of crime suspects, fleeing suspect interdiction and stolen property recovery.

The RPD respects privacy rights and will ensure its use of ALPR technology first and foremost protects those rights.

II. PURPOSE

The purpose of this policy is to provide RPD personnel with guidelines on the proper use of ALPR systems. The availability and use of ALPR systems have provided many opportunities for the enhancement of productivity, effectiveness and officer safety. It is the policy of the RPD that all members abide by the guidelines set forth herein when using ALPR systems.

III. DEFINITIONS

A. *FOUO*: For Official Use Only

B. *ALPR*: Automated License Plate Reader

C. *LPR:* License Plate Recognition

D. *Read*: Digital images of license plates, vehicles, and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the ALPR system.

E. *Alert*: A visual and/or auditory notice that is triggered when the ALPR system receives a potential "hit" on a license plate.

F. *Hit*: A read matched to a plate that has previously been registered on an agency's "hot list" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation, or which has been manually registered by a user for further investigation.

G. *Hot list*: License plate numbers of stolen cars, vehicles owned by persons of interest, vehicles used in the commission of crimes or related to identified crime suspects, vehicles associated with AMBER Alerts, etc. that are regularly added to "hot lists" circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the National Insurance Crime Bureau and the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. Law enforcement agencies can interface their own, locally compiled hot lists to the ALPR system. These lists serve an officer safety function as well as an investigatory purpose. In addition to agency supported hot lists, users may also manually add license plate numbers to hot lists in order to be alerted if and when a vehicle license plate of interest is "read" by the ALPR system.

H. *Fixed ALPR system*: ALPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

I. *Mobile ALPR system*: ALPR cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

J. *Portable ALPR system*: ALPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

K. *TCIC/NCIC:* Texas Crime Information Center / National Crime Information Center databases.

L. *TLETS*: Texas Law Enforcement Telecommunications System, which is a secure network through which access to TCIC/NCIC/ information is accessed.

IV. ADMINISTRATION

A. The CID Captain shall be responsible for managing all operations related to ALPR deployment and data control.

B. Access to data collected and retained by ALPR systems shall be in accordance with Criminal Justice Information Systems (CJIS) requirements and policies.

V. PROCEDURES

A. Use of an ALPR is restricted to the purposes outlined herein. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

B. An ALPR shall only be used for official law enforcement business.

C. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

D. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings, and other violent incidents, as well as serial or multi victim property crime events. Partial license plates reported during such crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

E. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

F. No ALPR operator may access department, state or federal data unless otherwise authorized to do so.

G. If practicable, officers should verify an ALPR response through TLETS before taking enforcement action that is based solely on an ALPR alert.

VI. ALPR DATA SHARING AND DISSEMINATION

A. ALPR data should be considered FOUO and can be shared for legitimate law enforcement purposes only.

B. All data and images gathered by an ALPR are for the official use of the RPD and because such data may contain confidential TLETS information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law. Dissemination of information to other law enforcement agencies outside Aransas County shall be made only in accordance with established MOUs or other written, working agreements or in accordance with this policy.

C. When ALPR data are disseminated outside the agency, it shall be with the approval of the CID Captain.

D. Information sharing among agencies should be dictated in accordance with MOUs (preferable for ongoing, long-term situations) or established departmental policies (in instances of short-term special investigations and similar events).

VII. ACCOUNTABILITY AND SAFEGUARDS

A. All saved data will be closely safeguarded and protected by both procedural and technological means. The RPD will observe the following safeguards regarding access to and use of stored data:

1. All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time;

2. Personnel approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action;

3. All ALPR data queries must be accompanied by the RPD case number corresponding with the investigation; without a case number entered, the system will not allow a query of license plate data; and

4. No entry of "hot lists" or other data may be entered into the ALPR database without the approval of the CID Captain.

B. The CID Captain shall audit the ALPR system at least quarterly, and the Chief will conduct an audit annually.

VIII. RETENTION

A. Data collected by RPD owned or leased ALPR equipment is owned by the RPD and will be retained for a maximum of 30 days.

B. ALPR data which has become, or it is reasonable to believe will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records shall be downloaded from the server onto portable media and booked into evidence.