

Title: Automated License Plate Reader (ALPR) Systems				
Date of Issue	Effective Date	Distribution	Amends/Rescinds	Review
12/18/2023	12/18/2023	B	New	12/18/2026
CFA Standards: 32.04		References:		
444.01 Purpose		444.04 Criteria for activation		
444.02 Definitions		444.05 Data sharing		
444.03 Training				
Policy: The availability of Automated License Plate Reader (ALPR) systems has provided many opportunities for the enhancement of productivity, effectiveness, and safety. As with any technology of this nature, it is incumbent upon law enforcement professionals to establish the necessary safeguards to instill public confidence the data and subsequent information gathered from the ALPR system(s) is/are used appropriately. It is the policy of the Gulfport Police Department (GPD) to ensure the ALPR system(s) and any information gathered as a result of the system operation, will be used for official and/or legitimate law enforcement purposes <u>ONLY</u> and privacy, civil rights, and liberties of individuals are not violated. ALPR systems are also known as License Plate Recognition (LPR) systems.				

444.01 Purpose: The purpose of this policy is to establish procedures, training, and guidelines for the use of automated license plate reader (ALPR) systems.

444.02 Definitions:

- A. Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest, also known as tag hits.
- B. Authorized user: An employee who has been approved to access the ALPR system by the designated ALPR administrator, after successfully completing the required agency-approved training.
- C. ALPR Coordinator: The agency member designated by the chief of police or his or her designee, to be the point of contact for ALPR systems. Requests for repair and/or replacement of ALPR equipment shall be directed to the ALPR coordinator who will coordinate with Flock Safety.
- D. ALPR system: A specialized system consisting of a camera(s) and computer software automatically recognizing the characters on vehicle license plates, comparing the data with law enforcement databases, and notifying users when there is a match. The ALPR will be permanently affixed in a stationary location to a pole. Flock Safety cameras are currently installed in the City of Gulfport. Flock Safety cameras do not retain Personally Identifiable Information (PII).
- E. Managed hotlists: Lists created by authorized users of the ALPR system that have a legitimate law enforcement purpose. Lists are categorized as “individual audience” or “organizational audience.” Individual audience lists notify the officer who entered the information of an ALPR capture. Organizational audience lists notify the agency of an

ALPR capture.

- F. Personally Identifiable Information (PII): Information that can be used to trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII includes names, gender, race, date of birth, photographs, addresses, social security numbers, driver's license numbers, or biometric data.
- G. System hotlist: The ALPR system integrates directly with 12 National Crime Information Center (NCIC) data files to provide alerts. System hotlists are maintained by the Florida Department of Law Enforcement and the Florida Department of Highway Safety and Motor Vehicles. The Panama City Police Department updates these hotlists eight times a day for NCIC entries and hourly for FCIC entries. Available system alerts include:
1. Canadian Police Information Center (CPIC) – records on property and vehicles that have been reported stolen in Canada.
 2. Gang file – records on violent gangs and their members.
 3. Immigration violator file – records on criminal aliens whom immigration authorities have deported and aliens with outstanding administrative warrants of removal.
 4. License plate file – records on stolen license plates.
 5. Missing persons file – records on individuals, including children, who have been reported missing to law enforcement and there is reasonable concern for their safety.
 6. National sex offender registry file – records on individuals who are required to register in a jurisdiction's sex offender registry.
 7. Protection order file – records on individuals whom protection orders have been issued against.
 8. Protective interest – records on individuals who might pose a threat to the physical safety of protected persons or their immediate families.
 9. Supervised release file – records on individuals on probation, parole, supervised release, released on their own recognizance, or during pre-trial sentencing.
 10. Vehicle file – records on stolen vehicles, vehicles involved in the commission of crimes, or vehicles that may be seized based on federally issued court orders.
 11. Violent person file – records on persons with a violent criminal history and persons who have previously threatened law enforcement. Data found within these record files are populated by agency users.
 12. Wanted person files – records on individual, including juveniles who will be tried as adults, for whom a federal warrant or a felony or misdemeanor warrant is outstanding.
- H. Tag detection: A digital record of a tag scanned by an ALPR and recorded in the corresponding database.
- I. Tag hit – An alert from the ALPR system that a scanned tag (tag detection) may be in the

National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, or terrorist-related activity.

- J. Target Alert Service (TAS): is a program that monitors designated ALPRs and alerts the user of a tag hit. The TAS is used to access tag hits detected by ALPR units monitored by the agency.

444.03 Training (CFA 32.04(A)).

- A. All authorized GPD users shall complete agency-approved training before utilizing or receiving system access to the ALPR system and must complete CJIS FCIC/NCIC limited access training.
- B. Training will be based on manufacturer recommendations, FCIC/NCIC regulation, and appropriate legal mandates and, at a minimum, will include in-service and field experience in the following:
 - 1. Proper use guidelines;
 - 2. Legal issues relating to the use, dissemination, and retention of data;
 - 3. Reporting requirements;
 - 4. Other topics/issues as deemed necessary and established by the agency.
- C. As part of the training, all members authorized to use the ALPR system are required to review and sign this written directive, which specifies privacy protections on the use of the technology and the impact and sanctions for potential violations.
- D. Training records will be maintained by the Office of Professional Standards.

444.04 Criteria for activation (CFA 32.04 (B)). ALPR technology is used for identifying and reading vehicle license plates that enter its “field of view” to capture the data/image associated with the plate. This system provides law enforcement with another useful tool that may be used for, but is not limited to: crime prevention/deterrence, criminal investigations, the apprehension of criminals, and the recovery of stolen property or missing persons.

- A. **Functionality:** ALPR cameras are motion-activated and capture the license plate of the vehicle while determining the make, model, and color via artificial intelligence software. Once a license plate is captured by the system, it is automatically compared to hotlists to provide an alert if necessary. These hotlists are not updated in real-time and any information obtained from them must be validated via an FCIC/NCIC query before law enforcement action can be taken. The ALPR system does not query FCIC or NCIC records. The system conducts comparisons of viewed tags.
- B. **Deployment:** ALPR cameras should be strategically deployed in areas of the City of Gulfport based on agency needs and are mounted in stationary/fixed locations.

- C. **Data privacy:** Searching stored ALPR data is conducted only by authorized members conducting an active investigation with the safeguarding of individual's privacy being of paramount concern.

444.05 Data Sharing (CFA 32.04 (C)).

A. User requirements and restrictions:

1. The use of ALPR systems and access to ALPR data requires a legitimate law enforcement purpose. No member may use or authorize the use of the LPR equipment or data for any other reason. Members must provide a report number/CAD log number in the search reason field for every search they conduct.
2. Members are subject to all policies and procedures applicable to the use of the ALPR system, including, but not limited to, the Criminal Justice Information Services (CJIS) procedures, the GPD information technology policies, and the records management maintenance and release policy. Additionally, members shall:
 - a. Possess a unique user identification to access the software, and set a unique password in the format outlined by the CJIS procedure password policy.
 - b. Not share his or her password, or otherwise provide access to the system to an unauthorized person.
 - c. Observe all FBI CJIS Security Awareness policies, GPD CJIS procedures, and other rules, written directives, and laws associated with the access to and use of personal identification information (PII).
 - i. Includes safeguarding against "shoulder surfing," or other unauthorized disclosure of information retrieved from the LPR system.
3. Misuse of ALPR equipment, associated databases, and/or data generated by the ALPR system will result in the user's access being suspended until retraining is completed, and may subject the user to corrective action, civil, and/or criminal penalties.
4. Authorized members will have the ability to query license plate recognition data, create reports, and use analytic tools, such as mapping capabilities.
5. GPD may share ALPR data with any government entity presenting an authorized law enforcement or public safety purpose.
6. GPD assumes no responsibility or liability for the acts or omissions of other agencies.
7. A hit by an ALPR system does not establish probable cause for an arrest or stop in and of itself. When a member discovers a "hit" it is his or her responsibility to confirm the hit is valid and is associated with the correct vehicle before taking any law enforcement action.

B. Access

1. Access to the ALPR system will be managed by the ALPR administrator or his or her designee.

2. Levels of access will be controlled based on the operational needs of the agency.
3. The ALPR administrator or his or her designee will manage the ALPR system accounts and filter access to program features on an as-needed basis.
4. Accounts will be granted for official use only.

C. Personal Identifying Information (PII)

1. Although the ALPR does not itself display or store PII, members should be mindful the license plate information provided offers a nexus through secondary searches to discovering PII of the registered owner and other individuals associated with the vehicle. In most cases, the information systems network members use to access both the ALPR software, other software, and databases storing PII are the same. For this reason, members will take the same precautions to protect the information entered, located, and retrieved from the ALPR system as he or she would with any other software or database connected to or accessed by the department's network.
2. Members shall treat all PII discovered from the ALPR searches and secondary searches of other software and databases using information retrieved from the ALPR system with the due regard required of Florida statute 817.568, the FBI CJIS Security Awareness policy and GPD's written directive 709 – Access to and Use of Secure Databases.

D. Retention of recordings (CFA 32.04 (D))

1. All data captured by the ALPR system is stored and maintained by the ALPR system vendor on a cloud-based (off-site) server.
2. The ALPR system vendor's server is authorized by CJIS, NCIC, and FCIC after confirmation it meets all applicable standards for maintenance, updating, and relaying secure criminal information.
3. Data is retained on the LPR system server for thirty (30) days. Any data needed for evidentiary purposes must be downloaded and logged as evidence in the applicable case.
4. Searches of data stored on the LPR system servers are subject to audit by the agency, including all searches conducted by the agency or by external agencies, who have been provided access to the data captured by GPD's ALPR system cameras.
5. The ALPR system vendor shall meet state and federal standards applicable for the retention of criminal information.
6. Retention will comply with all state and/or federal laws related to records use, security, dissemination, retention/destruction, and General Records Schedule GS-2, Item #217 – License Plate Recognition Records.

Mary Farrand
Chief of Police