

TALLAHASSEE POLICE DEPARTMENT

GENERAL ORDERS

 Proudly Policing Since 1826	SUBJECT Automated License Plate Recognition Systems		 Nationally Accredited 1986
	CHIEF OF POLICE <i>Signature on file</i>		
NUMBER 56	ORIGINAL ISSUE 05/12/2020	CURRENT REVISION 08/25/2026	TOTAL PAGES 8

This document contains information regarding technical and operational protocols that are protected under Public Records Laws. Seek guidance from the Legal Advisor prior to any release.

AUTHORITY/RELATED REFERENCES

FS Chapter 119, Public Records
 FS 316.0777, Automated License Plate Recognition Systems; ... Records Exemption
 FS 316.0778, Automated License Plate Recognition Systems; Records Retention
 General Records Schedule GS2 For Law Enforcement
 General Order 12, Radio Communications
 General Order 17, Records Management
 General Order 76, Traffic and Parking Enforcement
 General Order 77, Computer, Cellular Telephone and Data Utilization

ACCREDITATION REFERENCES

CALEA Chapter 41

KEY WORD INDEX

Annual Review Audit Requirements Confirming Hits Data Security and Access Data Storage and Retention General Information and Systems Description Guidelines for Use Member Training Prohibitions and Misuse Query Types	Procedure X Procedure IX Procedure IV Procedure V Procedure VII Procedure I Procedure III Procedure VI Procedure VIII Procedure II
--	---

POLICY

The Department is responsible for establishing clear protocols governing the use of Automated License Plate Recognition (ALPR) technology to enhance personnel's operational and investigative capabilities in support of crime prevention and the apprehension of criminal offenders. All authorized users shall adhere to these established protocols to ensure ALPR technology is utilized lawfully, effectively, and in a manner that supports community-focused public safety efforts.

PURPOSE

Automated License Plate Recognition (ALPR) systems support a community-centered approach to public safety by providing law enforcement with timely, accurate information to help identify and locate vehicles associated with criminal activity or critical incidents. ALPR technology is used as a focused investigative and crime-prevention tool to help recover missing or endangered individuals, respond more effectively to threats, and enhance overall community safety. Information obtained through ALPR may be used to support criminal investigations and other authorized law enforcement purposes. This technology is deployed under principles of transparency, accountability, and responsible data use to strengthen public trust and improve our community's quality of life.

DEFINITIONS

Confirmed Hit: A hit confirmed as valid and active by the original entering agency through FCIC/NCIC teletype.

Criminal Intelligence: Information collected by a criminal justice agency relating to an identifiable person, group of persons, vehicle, location, or business in an effort to anticipate, prevent, or monitor possible criminal activity when such information has been evaluated and determined to: 1) be relevant to the identification of criminal activity engaged in by an individual or organization reasonably suspected of involvement in criminal activity, and 2) meet criminal intelligence system submission criteria of the Department.

Hit: A visual and/or auditory alert triggered when the ALPR Systems receives a potential positive recognition of a license plate.

Hot List: A database list of license plates associated with motor vehicles and persons of interest as described in section II below.

Automated License Plate Recognition (ALPR) Program Administrator:

The ALPR Program Administrator is the designated Department representative responsible for overseeing the ALPR program's management, operation, and

compliance. Duties include maintaining user access controls, ensuring adherence to established protocols, coordinating audits, responding to complaints or allegations of misuse, and serving as the primary point of contact for program oversight, training, and system accountability. The Technical Operations Supervisor currently serves this role.

Automated License Plate Recognition (ALPR) Systems: The Department-approved systems designed to scan/read, store, and analyze license plate data, including the camera.

Tentative Hit: A hit which has been visually verified by the user against the Hot List and photograph, but has not yet been confirmed as valid and active.

PROCEDURES

I. GENERAL INFORMATION AND SYSTEMS DESCRIPTION

- A. Data and images gathered by the Automated License Plate Recognition (ALPR) Systems are for official Department use only and are considered active criminal intelligence.
- B. All data captured, stored, generated, or otherwise produced by an ALPR system are the property of the Tallahassee Police Department, regardless of where the data is housed or stored.
- C. The ALPR Systems passively capture and store a digital photograph of motor vehicles, focused on the license plate, entering its field of view, and compare the scanned license plate data to the Hot List (see section II below for query types) for matching information.

II. QUERY TYPES

- A. The Hot List query types may include, but are not necessarily limited to the following:
 - 1. Stolen motor vehicles,
 - 2. Stolen license plates,
 - 3. Suspended driver licenses,
 - 4. AMBER Alerts,
 - 5. Silver Alerts,

6. Vehicle or license plate of interest in criminal investigations, and
 7. U.S. Department of Homeland Security Watchlists.
- B. User-created Hot Lists are authorized solely for legitimate law enforcement purposes. Examples include, but are not limited to, vehicles or license plates associated with:
1. Habitual traffic offenders,
 2. Persons of interest or wanted persons in criminal investigations,
 3. Missing persons not meeting AMBER or Silver Alert criteria,
 4. Be On the Lookout (BOLO) notices,
 5. Attempt to locate persons (e.g., overdue motorist), and
 6. Registered sexual predators.

III. GUIDELINES FOR USE

- A. The only authorized utilization of the ALPR Systems is for legitimate law enforcement purposes.
- B. The use of the ALPR system requires the entry of a purpose and case number with each search.
- C. ALPR Systems may only be used to scan vehicle license plates in public view (i.e., plates of vehicles traveling or parked on any street or highway or other public property, or visible from a place or location where law enforcement has a legal right to be present).
- D. The ALPR Systems will be utilized and maintained in accordance with manufacturer recommendations.
- E. Only authorized members are permitted to utilize ALPR Systems.

IV. CONFIRMING HITS

- A. A tentative hit alone is not authority to make contact with an occupied motor vehicle (i.e., traffic stop or parked vehicle). A confirmed hit may not always provide authority to take enforcement action (i.e., confirming a vehicle hit is associated with a person of interest). Such instances will require independent

facts or circumstances providing for authority.

- B. Upon receipt of a hit, users shall contemporaneously visually compare the license plate information obtained by the ALPR Systems against the actual license plate displayed on the target motor vehicle to ensure they match.
- C. The user shall confirm the tentative hit with FCIC/NCIC via the Capital Region Real Time Crime Center (CRRTCC), MDC, or the CDA.
- D. When a tentative hit is the only known reason to make contact with an occupied motor vehicle (i.e., traffic stop or parked vehicle), officers shall not, except as noted in subsection E below, make the contact until the hit is a confirmed hit.
- E. Exigent circumstances and officer safety factors may necessitate action prior to hit confirmation.

V. DATA SECURITY AND ACCESS

- A. Users are responsible for the security of ALPR Systems data and shall only access, use, release, and/or disseminate such data for legitimate law enforcement purposes or per CJIS guidelines.
- B. Access to the ALPR Systems database shall be secured and controlled by the use of specific user login and password credentials capable of capturing and storing user access by date and time.
- C. Users shall only utilize their own credentials to access the ALPR Systems.

VI. MEMBER TRAINING

- A. Before members are granted ALPR Systems access, they shall complete Department-approved ALPR Systems training.
- B. The documented ALPR Systems training will include a policy review and may be provided via classroom or electronic presentation (e.g., e-mail, Power DMS).

VII. DATA STORAGE AND RETENTION

- A. Public records requests for ALPR Systems data shall be handled in compliance with General Order 17 (Records Management) and FS Chapter 119 (Public Records).
- B. The following protocols are applicable to the retention and disposal of all ALPR Systems data downloaded to the server:

TALLAHASSEE POLICE DEPARTMENT

1. Data shall be retained for a minimum of 30 days.
2. Data shall be retained and disposed of in accordance with the *General Records Schedule GS2 For Law Enforcement*, Item #217 (License Plate Recognition Records).
3. The Chief of Police or designee may set a shorter retention period.

VIII. PROHIBITIONS AND MISUSE

- A. Personnel are strictly prohibited from using Automated License Plate Reader (ALPR) systems, data, or associated equipment in any manner that is unauthorized, unethical, or inconsistent with law and Department policy. ALPR information shall be accessed and utilized only for legitimate law enforcement purposes directly related to official duties.
- B. The following actions are expressly prohibited:
 1. Accessing, retrieving, or reviewing ALPR data for personal interest, curiosity, or convenience.
 2. Using ALPR data to monitor individuals, vehicles, or locations without a valid law enforcement purpose.
 3. Sharing, disclosing, or disseminating ALPR data to any person or entity not authorized to receive such information.
 4. Altering, deleting, or falsifying ALPR records or system entries.
 5. Conducting searches intended to harass, intimidate, or target individuals or groups in violation of law or Department policy.
 6. Bypassing required access controls, authentication procedures, or audit mechanisms.
 7. Sharing login credentials, including usernames and passwords, with any other person. Each user is responsible for all activity conducted under their assigned credentials
- C. Any misuse of ALPR technology, data, or systems may result in administrative action, up to and including disciplinary measures, termination, and potential criminal arrest or civil liability. All personnel who become aware of suspected misuse shall immediately report the incident through the appropriate chain of command.

IX. AUDIT REQUIREMENTS

A. To ensure proper use, accuracy, and security of the Automated License Plate Reader (ALPR) system, the Department shall conduct routine audits of ALPR activity, data access, and system functionality. Audits verify compliance with legal mandates, Department policies, and authorized-use standards.

B. Audit Responsibility

1. The ALPR Program Administrator is responsible for coordinating and documenting all audits.
2. Any suspected misuse or policy violations discovered during an audit shall be immediately reported to the appropriate chain of command.

C. Audit Frequency

1. A monthly audit shall be conducted to review user access, query history, and any unusual or unauthorized activity. This monthly audit shall be forwarded through the appropriate chain of command to the Administration/Investigations Deputy Chief of Police.
2. A complaint or allegation of misuse of ALPR may trigger an immediate audit focused on the relevant user activity and system logs.
3. An annual comprehensive audit shall be conducted to evaluate system performance, adherence to policy, and the effectiveness of privacy and security safeguards. This audit shall be forwarded through the appropriate chain of command to the Administration/Investigations Deputy Chief of Police.

D. Audit Scope

Audits may include, but are not limited to:

1. User access logs, including frequency and purpose of searches.
2. ALPR data queries, hit confirmations, and investigative follow-up documentation.
3. Verification that searches and data access are linked to legitimate law enforcement activity.

TALLAHASSEE POLICE DEPARTMENT

4. Review of data retention, automatic purge cycles, and storage compliance.
5. System configuration changes, administrative permissions, and security controls.
6. Any anomalies, irregular patterns, or attempted unauthorized access.

X. ANNUAL REVIEW

This policy will be reviewed each year during the annual audit. After the audit and any needed revisions, the policy will be sent to all applicable members for annual review.

History: Issued 05/12/2020.