

DICKENSON COUNTY SHERIFF'S OFFICE		132
GENERAL ORDERS		
	SUBJECT Automated License Plate Reader (ALPR) Policy	EFFECTIVE DATE January 26, 2026
	CHAPTER Operations	REVISED DATE August 28, 2026
APPROVED: 		Jeremy D. Fleming, Sheriff
VLEPSC: OPR 02.02, OPR 02.04, OPR 06.01, OPR 08.01, OPR 08.03, OPR 08.05, OPR 09.01		

NOTE: This directive is for internal use only and does not enlarge a Deputy's civil or criminal liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this directive, if proven, can only form the basis of a complaint by this department, and then only in a non-judicial administrative setting.

I. PURPOSE

The purpose of this policy is to establish guidelines governing the use of Automated License Plate Reader (ALPR) technology by the Dickenson County Sheriff's Office (DCSO). This policy is intended to ensure that ALPR systems are used in a lawful, responsible, and transparent manner consistent with the Code of Virginia § 2.2-5517 and applicable constitutional protections.

II. AUTHORITY AND OVERSIGHT

The Sheriff of Dickenson County, or a designated command staff member, shall have overall responsibility for the administration and oversight of the Automated License Plate Reader (ALPR) program.

Oversight responsibilities include approving authorized users, ensuring required training is completed, ensuring compliance with this policy and applicable law, and conducting or delegating required internal audits.

III. DEFINITIONS

For purposes of this policy, the following definitions apply:

- **Automated License Plate Reader (ALPR):** A system of one or more cameras used in combination with computer algorithms to capture images of license plates or vehicles and convert those images into computer-readable data.
- **ALPR System Data:** All data collected or generated by the ALPR system, including images, license plate numbers, vehicle descriptions, and associated date, time, and location information.
- **Audit Trail:** Records documenting each access, query, or use of the ALPR system, including user identity, date and time of access, purpose of access, and associated incident or case number.

- **Notification:** An alert generated by the ALPR system indicating a potential match between captured data and a database or hotlist.

IV. AUTHORIZED USES

The ALPR system may only be used for the following purposes, as authorized by § 2.2-5517(D):

1. As part of a criminal investigation where there is reasonable suspicion that a violation of the Code of Virginia or local ordinance has occurred.
2. As part of an active investigation involving a missing or endangered person.
3. As part of an investigation involving a person associated with human trafficking.
4. To receive and review notifications related to:
 - Missing or endangered persons
 - Persons with outstanding warrants
 - Stolen vehicles
 - Stolen license plates

The ALPR system shall not be used for general surveillance, intelligence gathering unrelated to a specific authorized purpose, or to monitor individuals engaged in lawful activity.

V. PROHIBITED USES

ALPR systems shall not be used:

- To track individuals based solely on lawful activity or protected speech.
- For non-criminal justice purposes.
- To enforce traffic laws such as parking violations, speed enforcement, tolling, or emissions monitoring.
- For personal, political, or discriminatory purposes.

VI. TRAINING REQUIREMENTS (§ 2.2-5517(H)(1))

Only sworn personnel or authorized employees who have completed required ALPR training and have been authorized by the Sheriff or designee may access or use the ALPR system.

ALPR training shall include instruction on lawful use, system operation, data retention requirements, privacy considerations, and documentation and audit requirements.

Operational training on the ALPR system shall be completed through vendor-provided training resources associated with the ALPR system in use. Completion of such training shall be documented through vendor-maintained training records or transcripts.

In addition, all authorized users shall review and acknowledge this policy through the agency's policy management system prior to accessing the ALPR system.

Refresher training shall be provided as necessary or when changes in law, policy, or system functionality occur.

VII. DATABASE UPDATES (§ 2.2-5517(H)(3))

Databases and hotlists used by the ALPR system to generate notifications shall be updated at least every 24 hours, or as soon as practicable after updates become available.

The Dickenson County Sheriff's Office relies on vendor-managed and system-integrated update processes to ensure that external databases and comparison lists are refreshed in accordance with this requirement.

Any agency-created or agency-uploaded hotlists shall be reviewed as necessary to ensure accuracy and shall be removed or updated when no longer accurate or necessary.

The Sheriff or designee shall ensure that procedures are in place to verify that database update mechanisms are functioning as intended.

VIII. VERIFICATION PRIOR TO VEHICLE STOPS (§ 2.2-5517(H)(4) & (M))

An ALPR notification alone does not constitute reasonable suspicion for a vehicle stop. Prior to initiating a stop based on an ALPR notification, an officer shall:

1. Develop independent reasonable suspicion; or
2. Confirm that the license plate or vehicle characteristics match the information contained in the database that generated the notification.

Verification steps and outcomes shall be documented in the associated incident or case report.

IX. DATA ACCESS AND DOWNLOAD RESTRICTIONS (§ 2.2-5517(H)(5))

ALPR system data shall not be accessed, queried, or downloaded unless directly related to an authorized purpose listed in this policy. Downloading system data is prohibited except when necessary for a lawful investigation, audit, or court proceeding.

X. DATA RETENTION AND DESTRUCTION (§ 2.2-5517(H)(7))

ALPR system data shall be retained for no longer than 21 days from the date of capture, unless the data is related to an ongoing investigation, prosecution, or court proceeding. Audit trail data shall be retained for at least two years.

Data shall be purged in a manner that renders it unrecoverable, consistent with vendor capabilities and applicable records retention laws.

XI. DATA SHARING AND DISCLOSURE (§ 2.2-5517(H)(8))

ALPR system data and audit trail data shall not be sold or shared except as authorized by law. Authorized sharing is limited to:

- Other law enforcement agencies for lawful investigative purposes
- The Commonwealth's Attorney or defense counsel as required by law
- Court orders or subpoenas
- The system vendor for maintenance or quality assurance purposes

All sharing shall be documented.

XII. INTERNAL AUDITING (§ 2.2-5517(H)(6))

The Dickenson County Sheriff's Office shall conduct an internal audit of ALPR use at least once every 30 days. Audits shall review compliance with this policy, documentation accuracy, and authorized use. Audit results shall be documented and retained.

XIII. SECURITY SAFEGUARDS (§ 2.2-5517(H)(9))

The ALPR system, system data, and audit trail data shall be protected against unauthorized access, use, modification, destruction, or disclosure. Security measures include role-based access controls, user authentication, activity logging, and prompt deactivation of access upon separation or reassignment.

XIV. VIOLATIONS AND SANCTIONS

Any employee who knowingly or intentionally uses the ALPR system in violation of this policy or applicable law may be subject to disciplinary action, criminal prosecution, or both.

XV. POLICY REVIEW

This policy shall be reviewed periodically and updated as necessary to ensure continued compliance with applicable law and best practices.