AUTOMATIC LICENSE PLATE RECOGNITION USE REQUIREMENTS

Pursuant to, and in accordance with, COV §2.2-5517, *Use of automatic license plate recognition systems by law-enforcement agencies* and Operating Procedure 030.4, *Office of Law Enforcement Services*, the Virginia Department of Corrections, Office of Law Enforcement Services (OLES), is authorized to utilize automated license plate recognition (ALPR) equipment systems to support official law enforcement activities. This technology will be used to enhance public safety through effective, responsible data collection and usage only.

ALPR equipment will be operated in compliance with federal and state laws, local ordinances, and The Commission on Accreditation for Law Enforcement Agencies (CALEA) standards, specifically ensuring the integrity, security, and lawful use of collected digital information. This attachment outlines requirements related to ALPR training, use, data governance, and public transparency.

DEFINITIONS

Audit Trail - All records of queries and responses in an automatic license plate recognition system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the:

- date and time of access;
- license plate number or other data elements used to query the system;
- specific purpose for accessing or querying the system, including the offense type for any criminal investigation;
- associated call for service or case number; and
- username of the person or persons who accessed or queried the system.

Authorized User - A trained and approved staff member with documented authorization from the Chief of Law Enforcement Services to access ALPR data for official purposes.

Hot List – A list of license plate numbers flagged due to letters of stolen cars, vehicles owned by persons of interest, or vehicles associated with AMBER Alerts.

Notification - An alert from an ALPR system that a license plate or vehicle matches a license plate or vehicle in a database utilized by the ALPR system for comparison purposes.

System Data - All forms of data collected or generated by an ALPR system, including images of license plates, vehicles, any identifying characteristics of vehicles, the date, time, and location of an image, and any peripheral images collected from which analytical data may be extracted.

I. PRIVACY SAFEGUARDS

A. The use of ALPR technology is limited to official law enforcement objectives and may not infringe on individual privacy rights.

B. ALPR technology may be used for:

1. locating vehicles involved in crimes;
2. locating stolen vehicles or missing persons;
3. supporting BOLOs, AMBER/Silver Alerts:
4. identifying vehicles of interest related to court orders or warrants; or
5. other criminal investigations.

C. ALPR technology may not be used for:

1. general surveillance without connection to criminal activity;
2. traffic citations or civil enforcement;
3. immigration status investigations; or
4. personal interest or non-official activities.

D. All bulk data access requests must be reviewed and approved by the Chief of Law Enforcement Services or their designee.

II. SYSTEM ACCESS AND AUTHORIZATION

A. Access to ALPR data is restricted to authorized users.

1. Authorized user credentials must be unique and traceable.
2. System usage must be logged.
3. Unauthorized access, sharing, or copying of ALPR data is prohibited.
4. All access to the ALPR system shall be recorded in an audit trail that includes:
   a. date and time of access;
   b. full or partial license plate queried;
   c. purpose of the query (aligned with an authorized law enforcement purpose);
   d. associated case or service call number; and
   e. username of the authorized user.
5. Any data-sharing arrangements with external agencies must be governed by formal Memoranda of Understanding (MOUs) and tracked for audit compliance.
6. OLES will maintain communication with the ALPR technology provider to ensure system security, firmware updates, and alignment with contractual service-level expectations.

III. TRAINING REQUIREMENTS

A. All authorized users must complete initial and bi-annual training on:

1. ALPR system operation;
2. appropriate use requirements; and
3. statutory use restrictions including:
   a. required data entry for audit trails;
   b. appropriate query purposes; and
   c. public reporting requirements.

B. Documentation of training must be maintained in each user's personnel file.

IV. HOT LIST MANAGEMENT

A. The ALPR system will compare captured license plate data against system hot lists to identify vehicles of interest.

B. All hot lists used by OLES must be current, validated, and updated in compliance with COV §2.2-5517, *Use of automatic license plate recognition systems by law-enforcement agencies*.

C. Manually entered license plates will include required supporting information and be maintained for investigatory purposes only.

V. VEHICLE STOP PROCEDURES AND REPORTING

A. All enforcement actions based on ALPR system notifications must be conducted in strict compliance with Virginia law, including COV §2.2-5517, *Use of automatic license plate recognition systems by law-enforcement agencies* and COV §52-30.2, *Prohibited practices; collection of data*.

B. Vehicle Stop Validation

1. A notification from the ALPR system does not, by itself, constitute reasonable suspicion or probable cause to conduct a traffic stop. Prior to initiating any enforcement action, the OLES Agent must:
   a. develop independent reasonable suspicion to justify the stop; or
   b. confirm that the license plate and vehicle characteristics (e.g., make, model, color) observed match those listed in the ALPR system and hot list used to generate the alert.
      i. Confirmation must include an independent verification of the ALPR system alert against the corresponding hot list entry.
      ii. OLES Agents are strongly encouraged to use radio communications or mobile terminals to validate alert information in real time.

C. Traffic Stop Reporting Requirements

1. If an officer performs any of the following based on an ALPR alert, the OLES Agent must comply with the reporting requirements established under COV §52-30.2, *Prohibited practices; collection of data*:
   a. a traffic stop of a motor vehicle;
   b. a stop and frisk of a person; or
   c. a temporary detention of any individual.
2. If the above policing actions are performed, the following information must be documented:
   a. the reason for the stop or detention;
   b. the location, date, and time of the action;
   c. the race, gender, and age of the person stopped or detained, if known;
   d. whether a search was conducted; and
   e. whether any warning, citation, or arrest occurred.

D. All such documentation must be submitted using the designated reporting platform or form adopted by the Virginia Department of Criminal Justice Services (DCJS), and copies must be retained in the case record.

VI. DATA RETENTION AND SECURITY

A. ALPR data must be stored securely on the ALPR platform.

B. Passive data not linked to an alert, investigation, or criminal activity may not be accessed, analyzed, or retained beyond the authorized retention period.

C. Data will be automatically purged after 21 days unless flagged for an ongoing investigation or legal hold in accordance with Operating Procedure 030.1, *Evidence Collection and Preservation*.

D. Audit trail data must be retained for two years from the date of capture.

1. Once the two-year retention period is complete, audit trail data will be purged in a manner that renders it unrecoverable by the vendor or the agency.
2. The purge may be deferred if the audit trail data is part of an active investigation, prosecution, or civil proceeding,

E. Misuse of data includes but is not limited to:

1. accessing ALPR data for personal reasons;
2. searching without an official case number or lawful justification; or
3. sharing data outside of authorized channels.

F. All data violations will be documented and reported to agency leadership and, where required, external oversight bodies.

G. Confirmed misuse may result in disciplinary action up to and including termination and may be referred for criminal prosecution.

H. Data encryption and system integrity are maintained by the vendor and subject to agency oversight.

VII. PUBLIC DATA REQUESTS

A. All public data requests must be reviewed for compliance with COV §2.2-3700 et seq., *The Virginia Freedom of Information Act* and will exclude sensitive investigative information.

B. System data and audit trail data will not be subject to disclosure under COV §2.2-3700 et seq., *The Virginia Freedom of Information Act*.

C. Requests for ALPR safety reports or metrics will be addressed in accordance with:

1. agency transparency and confidentiality policies;
2. data retention and privacy guidelines; and
3. CALEA-aligned mobile data standards.

D. OLES may not share system data or audit trail data with, or disseminate such data to, a database of any other state, federal, private, or commercial entity.

E. OLES may not sell any system data or audit trail data.

VIII. AUDIT, ACCOUNTABILITY AND REVIEW

A. All system activity is logged and subject to internal audit by the Director or their designee.

B. All ALPR data requests and alerts must be documented with a case number or reason.

C. Misuse or violation of ALPR use requirements may result in disciplinary action and reporting to

oversight bodies.

D. Audits will be conducted every 30 days to ensure system access, queries, and data usage align with established use requirements.

E. Audits must consist of:

1. at least 5% of queries, downloads, and stops; and
2. monthly verification of agency sharing settings.

F. Audit documentation must be maintained for compliance records.

IX. TRANSPARENCY AND PUBLIC REPORTING

A. The Chief of OLES will issue a summary report annually, including:

1. the number of alerts and matches;
2. criminal investigations supported;
3. any misuse or access violations;
4. the number of cameras in use by type (vehicle-mounted, fixed, temporary);
5. the total number of system queries and purpose;
6. the number of vehicle stops based on alerts and reasons;
7. demographic data (race, gender, ethnicity, age) of people stopped and charged;
8. any data shared with external agencies;
9. the number of unauthorized access incidents; and
10. the number of subpoenas, search warrants, and data requests received.

B. The Chief of OLES will publicly post the annual report and the ALPR use requirements on the agency's website, excluding any data that is sensitive, personally identifiable, or protected by law.

C. A copy of the annual report will be provided to the CALEA Accreditation Manager.

X. VENDOR AND CONTRACT REQUIREMENTS

A. Any vendor contracted for ALPR services must:

1. certify that system and audit trail data will not be sold, shared, or accessed without agency request;
2. comply with a 21-day purge policy for system data and a two-year retention period for audit trail data;
3. maintain security protocols that meet Virginia Information Technologies Agency (VITA) standards;
4. immediately notify OLES upon receipt of any subpoena, search warrant, or third-party request for data, unless prohibited by law; and
5. ensure all data remains the sole property of OLES and the Virginia Department of Corrections (DOC).

XI. INSTALLATION, INFRASTRUCTURE COMPLIANCE, AND NOTICE OF USE

A. If installed on Commonwealth-controlled rights-of-way, OLES will comply with the Virginia Department of Transportation (VDOT) permitting requirements in accordance with COV §2.2-5517(Q).

B. All installations will conform to the regulations of the Commonwealth Transportation Board and any conditions required for such permits.

C. Signs must be posted at all state facilities and offices indicating that ALPR Technology may be in use and that all persons may be subject to audio and video recording.

1. Where the entire premises are owned or occupied by the DOC, signs shall be displayed at every entrance.
2. Where only a portion of the premises are leased for use by the DOC, the signs shall be displayed within the leased space.