Subject: Automated License Plate Readers		Policy Number: OPR: 50
Revision Number: 1	Effective Date: 01/28/2025	Original Issue Date: 04/09/2018

1) PURPOSE

a) This policy establishes the authorized use, operational guidelines, and capture, of digital data collected through the Automatic License Plate Reader Program.

2) POLICY

a) It is the policy of the Department of Public Safety to explore new technologies that advance the capabilities of the department to protect and serve the public. This policy is designed to provide guidance in the use of ALPRs and the retention, dissemination and disposition of the data they generate, while continuing to safeguard the right of privacy of the public.

3) APPLICABILITY

a) This policy applies to all DPS personnel.

4) REFERENCES

a) **CALEA 41.3.9 License Plate Recognition Systems**
b) **NMAC 1.21.2.507 Retention of Transportation and Trip Permits.**
c) **CIJIS Security Policy Version 6.0**

5) DEFINITIONS

a) **Automated License Plate Reader (ALPR) –** An electronic device that is capable of photographing a vehicle and/or its license plate identifying alpha-numeric characters and comparing the collected data and photographs to existing law enforcement databases for investigative purposes.
b) **Alert –** an audio-visual notice that is triggered when the LPR system receives a potential "hit" on a license plate.
c) **ALPR Data -** Digital data captured by the ALPR in the form of an image (such as a license plate or description of a vehicle on which it is displayed) within public view. Information captured by the device includes GPS coordinates,

license plate number, vehicle make and model, and time the information was captured by the ALPR system. All ALPR data is considered CJIS (Criminal Justice Information Services) data, meaning it falls under the regulations and security standards set by the FBI for criminal justice information sharing; therefore, access and usage of LPR data by all users must comply with CJIS policies.

d) **Authorized User –** A Commissioned Officer, Transportation Inspector, Communication Bureau Specialist, or other DPS employee who has successfully completed training on ALPR policy, has passed an NCIC Certification Exam, is trained on the operation of equipment and systems related to ALPR, and has approved access or use of the DPS ALPR Systems **through a user specific account. All Authorized ALPR users must complete the CJIS Security Awareness training and testing annually.**

e) **Authorized Administrator -** A DPS employee who has successfully completed advanced training on ALPR and CJIS policy, has passed an advanced NCIC Certification Exam, is trained on the administration of the systems related to ALPR, and has approved access **through a user specific account with elevated privileges. All Authorized ALPR users must complete the CJIS Security Awareness training and testing annually.**

f) **Hot List –** A specific list entered by a law enforcement agency: including but not limited to, vehicles which are reported as stolen, display stolen license plates, vehicles of interest for criminal investigations, vehicles with an articulable criminal nexus or valid public safety concern, including vehicles which are reported as used in the commission of a violent crime, property crime, vehicles linked to missing persons and/or wanted persons and vehicles flagged by law enforcement agencies for officer safety concerns.

g) **Hit –** An alert from the ALPR system that a scanned license plate number may be in NCIC or other law enforcement database for a specific reason including, but not limited to, being related to a stolen vehicle, stolen license plate, wanted person, AMBER Alert, missing person or terrorist-related activity.

h) **NCIC –** National Crime Information Center (NCIC) is a computerized index of missing persons and criminal information and is designed for the rapid exchange of information between criminal justice agencies.

i) **Read –** A record of a license plate scanned by an ALPR camera that includes an image of the vehicle and plate, along with the plate characters, date and time of the scan and GPS location of the scan.

j) **FMCSA (Federal Motor Carrier Safety Administration) -** a database that regulates and provides safety oversight of commercial motor vehicles.

6) OPERATIONAL PROCEDURES

a) **Usage**

i) Use of the ALPR system is restricted to the purposes outlined within this policy and training.

(1) Information gathered or collected, and records retained by the department ALPR system will not be accessed or used for any reason other than legitimate law enforcement or public safety purposes.

(2) Department personnel shall not use, or allow others to use, ALPR equipment or database records for any unauthorized purpose. Department personnel shall only access LPR data via their own unique log-in.

ii) The following uses of the ALPR system are specifically prohibited and are considered unauthorized:

(1) Invasion of Privacy: Except when done pursuant to a court order or search warrant, it is a violation of this policy to utilize an ALPR to record license plates except of those vehicles which are exposed to public view (i.e. vehicles on a public road; or parked on private property with the license plate visible from a public road, street or where members of the public have access to, such as a parking lot of a business).

(2) Harassment or Intimidation: It is a violation of this policy to use an ALPR system, or information contained therein, to harass or intimidate any individual or group.

(3) Personal Use: It is a violation of this policy to use an ALPR system or associated digital data or hot lists for any personal use.

iii) Valid CAD or Case Numbers shall be entered for all hot plate entries and plate searches within the ALPR database.

iv) All LPR hits utilized to conduct or initiate enforcement action shall be downloaded from the ALPR system and retained as evidence within the department's digital evidence management system (DEMS) where the record shall be tagged with a case number.

b) **Administration**

i) The Chief will designate an ALPR Administrator. This administrator shall have oversight of system operations to include overseeing the maintenance, installation, system access and data retention. This administrator shall:
   (1) Establish protocols for access, collection, storage of ALPR data and associated data.
   (2) Establish protocols to preserve and document ALPR alerts, hits or hot lists which are acted upon through investigations or prosecutions.
   (3) Establish protocols to monitor the ALPR system database to ensure the security and integrity of data captured, stored, and/or retained by vendor ALPR systems and information complies with applicable privacy laws.
   (4) Establish training requirements for department personnel to operate the ALPR system by coordinating with the Advanced Training Bureau.
   (5) Maintain records identifying approved physical ALPR deployment locations and documenting results, including documentation of incidents deemed significant by the Chief, or designee, and arrests related to ALPR usage.
   (6) Authorize or deny any requests for ALPR data access by outside agencies through consultation with the Chief, or designee.
   (7) Ensure ALPR system access, and all data and images gathered by the system, shall be for official use only. To facilitate proper operation and oversight of the system, any database or user lists will have the ability to be audited.
   (8) Personnel will be assigned access to the digital storage application appropriate to their rank and/or duties.
   (9) The Department of Public Safety shall maintain detailed audit logs for all access and usage activities, including user ID, time, and actions.
   (10) The administrator shall conduct quarterly reviews of audit logs to detect unauthorized access or unusual activity. If the Administrator identifies logging failures, the authorized personnel first line supervisor will be notified immediately.
   (11) If any authorized personnel identify a security breach, the Administrator shall be notified immediately. The Administrator shall notify IT Support Cyber Security Division within 24 hours of the security breach, so the security breach can be contained. A root

cause analysis of the security breach will be conducted by the IT Support Cyber Security Personnel.

c) **Access Control**

i) Authorized personnel:

(1) Administrator: The administrator shall oversee system operations, including maintenance, installation, system access, and data retention.

(2) Officer/Agent: Those employees, regardless of rank, who are sworn peace officers of the New Mexico State Police.

(3) IT Support: Technology Support staff employed by the Department of Public Safety, who will assist the Administrator with the maintenance and system operations.

(4) Communications Personnel: Communications Bureau staff employed by the Department of Public Safety who have access to NCIC sensitive material.

(5) Transportation Inspectors: Personnel employed by the Department of Public Safety who conduct commercial vehicle inspections and enforcement on commercial motor vehicles.

ii) Limit access to sensitive data (e.g., Hot Lists, case-related data) to authorized personnel only.

(1) Require Multi-Factor Authentication for all users accessing ALPR systems or data to enhance authentication security in compliance with the current vendor and DPS protocols.

d) **Training**

i) Personnel will be trained in the use of the ALPR system and the associated equipment prior to accessing system information.

ii) Conduct annual training for all personnel on CJIS-compliant data security practices.

iii) Provide role-specific training for ALPR administrators and users with elevated access privileges.

iv) Update training materials after policy changes or security incidents.

e) **Duties of Personnel**

i) Personnel may access the ALPR systems to further law enforcement investigations. Each user is required to have individual credentials for access and use of the ALPR system and/or associated data.

ii) Personnel may view, review, and share their own ALPR data with other personnel to further an investigation, ensure system accuracy or quality. The information can be used for reports and law enforcement interviews.

iii) The information contained within the system must be treated as confidential and used as an investigative lead only. Any investigative leads generated must be vetted by department personnel through a normal investigative process for inclusion into a case folder within the department approved Digital Evidence Management System.

iv) Personnel shall:

(1) Ensure their assigned ALPR is functioning properly at the beginning of each shift according to the instructions of the system's manufacturer.

(2) Immediately report any malfunctioning equipment to a supervisor. Any repairs or modifications to ALPR equipment or systems shall only be accomplished by authorized technicians or vendors as determined by the ALPR administrator.

(3) Confirm the license plate from an alert matches the license plate on the observed vehicle and verify the validity of the alert through NCIC or FMCA prior to initiating a law enforcement encounter or investigation.

(4) Convert LPR hits utilized to conduct enforcement action to evidence and store them in the department's digital evidence management system, tagged with the relevant case number.

v) An ALPR will be installed in a department vehicle as determined by the NMSP command staff. The NMSP command staff must pre-approve the transfer of an ALPR unit to another area. Otherwise, if an employee who is assigned a vehicle equipped with an ALPR is transferred, promoted, or resigns, the vehicle will be reassigned to another employee in the unit's designated area.

vi) Department personnel accessing the ALPR database to search for information must enter a valid reason for the inquiry and the associated case or CAD event number. Use of generic reasoning (i.e. 'investigation' or 'research') when searching an ALPR database is prohibited.

vii) Any call for service generated from a system alert through dispatch will be assigned to a call for service type noting that the call for service is

related to an LPR hit. **If an Officer/Agent/Inspector gets a system alert, the Officer/Agent/ Inspector will notify dispatch so the system alert can be added to the call for service**. Should any personnel receive an ALPR Alert, the operator will verify the ALPR hit through NCIC or FMCA. Prior to the closing of the call for service the Officer/Inspector/Agent shall notify dispatch of the final disposition of the call, so the proper documentation is accurately reflected. **Dispositions will be thorough and notate all enforcement actions**.

f) **Supervisor Responsibilities**

i) In addition to the above responsibilities, supervisors shall:

(1) Review the Hot List entry requests from Officers, Agents, and Inspectors under their supervision for validity before entry and removal from the system.

(2) Report equipment problems to the ALPR administrator and seek to have equipment immediately repaired or replaced as needed.

(3) Supervisors shall investigate, and discipline assigned personnel who intentionally, unjustifiably or display a pattern of using an ALPR system in an unauthorized manner. Supervisors will report any documented incidents of violation to the CJIS Chief Security Officer for an incident response.

g) **Non-Compliance Penalties**

i) Employee failure to follow ALPR use and duty policy will result in progressive discipline handled within the chain of command and the following progressive penalties recorded and issued by the ALPR Administrator:

(1) First offense: Revocation of ALPR system access for 15 days.

(2) Second Offense: Revocation of ALPR system access for 30 days.

(3) Third Offense: Permanent revocation of ALPR system access.

System access revocations will be based on a review of administrative penalties for the prior 365 calendar days. After 365 days of compliance an employee will be assessed on a clean slate.

h) **Redaction, Retention, and Release**

i) The Department of Public Safety will comply with all existing laws and regulations governing retention and disclosure of public information.

ii) Hit and Read records will be stored on a dedicated media storage system through the approved vendor for a period of no less than 30 days if there are no subsequent ALPR hits through NCIC. Any images generating a subsequent ALPR Hit through NCIC shall be retained for a period of no less than 180 days. Hit records utilized in enforcement action will be retained as evidence in the agency's digital evidence management system until the adjudication of a case and deleted only after obtaining a destruction order.

iii) Accessing, copying, or releasing ALPR images for non-law enforcement purposes is strictly prohibited unless authorized by law and approved by the Chief or designee.

iv) Department of Public Safety personnel including DPS I.T. personnel, IPRA personnel and administrative personnel, must reasonably safeguard all digital images associated with the ALPR system. Personnel are accountable for the appropriate security and retrieval of items of evidence to ensure the proper chain of custody is documented for potential court proceedings.

i) **Encryption and Secure Transmission**

i) The Department of Public Safety shall require AES-256 encryption for all ALPR date stored at rest.

ii) The Department of Public Safety shall use TLS 1.2 or higher to secure data in transit between devices and storage systems.

j) **Intentional Manipulation**

i) Personnel will not tamper, alter, edit, erase, duplicate, share, disseminate, or manipulate any ALPR images or metadata. This includes intentionally positioning or obscuring the assigned ALPR camera so that the law enforcement or investigative encounter is not captured by the camera. Such intentional acts will result in disciplinary action to include termination. Personnel shall not attempt to physically alter the ALPR camera.

7) ATTACHMENTS

a) **NONE**

8) APPROVAL

APPROVED BY: s/Jason R. Bowie **DATE:** January 28, 2025
DPS Cabinet Secretary