	ANCHORAGE POLICE DEPARTMENT POLICY AND PROCEDURE	Distribution ALL PERSONNEL	Policy Number **7.12**
		Previous Issue Date MM/DD/YY	Reissue/Effective Date MM/DD/YY
Policy Title: **AUTOMATED LICENSE PLATE READERS (ALPR)**		Accreditation Standard:	Section 7
		Rescinds:	
Section Title: SPECIAL OPERATIONS		**Sean Case, Chief of Police**	

This Policy is for departmental use only and does not apply in any criminal or civil proceeding. This Policy should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this Policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.

I. PURPOSE

To provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

II. POLICY

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection and number recognition of license plates. It is the policy of the Anchorage Police Department (Department) to utilize ALPR technology to capture digital license plate data and images while recognizing the established right to privacy in Alaska. Data captured by ALPRs serve two purposes; first, the immediate detection of stolen or wanted vehicles, vehicles associated with missing persons, vehicles and/or vehicles owners involved in violent crime, and vehicles and/or vehicles owners involved in drug distribution; and second, as an investigative tool during the course of an investigation. Captured data will only be stored for a limited amount of time before it is deleted. ALPR data will not be available for crimes that are reported after the retention period has expired.

III. DEFINITIONS

Automated License Plate Reader (ALPR): Specialized camera system that automatically captures and processes images of vehicle license plates using optical character recognition (OCR). These systems can identify plate numbers in real time or from recorded footage, and cross-reference them against databases to assist with law enforcement, traffic management, and security operations.

Detection: Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the ALPR, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location at the time of the ALPR's read.

Digital Multimedia Evidence (DME): Digital recording of images, sounds, and associated data.

Hit: Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC), APSIN (Alaska Public Safet Network), or Department database for a specific reason including, but not limited to, being related to a stolen car, missing person, or a suspect in a violent crime.

Hot List: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, APSIN, RMS (Records Management System), Silver and Amber Alerts, etc.

Optical Character Recognition (OCR): Technology that converts images of printed, typed, or handwritten text into machine-readable digital text. It uses pattern recognition and artificial intelligence to identify characters in scanned documents, photographs, or video frames, enabling the text to be edited, searched, and stored electronically

Real Time Crime Center (RTCC): A centralized law enforcement element that integrates live camera feeds, public safety data, and analytical technologies to provide immediate operational intelligence. It functions to support rapid response to crimes in progress, enhance situational awareness, and facilitate public safety.

Vehicles of Interest: Including, but not limited to vehicles that are stolen, associated with missing persons, vehicles and/or vehicles owners involved in violent crime, and vehicles and/or vehicles owners involved in drug distribution.

IV. PROCEDURE

A. Program Overview

1. Department employees shall not use or allow others to use the equipment or database records for any unauthorized purpose.
2. An ALPR shall only be used for official law enforcement business. Any employee using ALPR data for any purpose other than investigating a criminal offense is subject to discipline.
3. No Department employee shall operate ALPR equipment or access ALPR data without first completing Department approved training.

B. Operational Objectives

1. Identify stolen vehicles.
2. Locating vehicles associated with criminal investigations.
3. Supporting Amber/Silver Alerts and missing person cases.
4. Real-Time Crime Center (RTCC) operations for immediate investigative leads.

C. General Operations

1. Officers, Dispatch, and/or RTCC employees shall verify an ALPR response through APSIN before taking enforcement action. A hit does not come directly from APSIN, requiring verification prior to taking police action.
2. Once an alert is received, officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the

ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding.

3. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are responsible for ensuring they have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. For example, if a vehicle is entered into the system because of its association with a wanted individual, officers should visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.
4. Verification of status on a hot list. An officer must receive confirmation, from Dispatch or other Department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

D. Prohibited Use

1. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).
2. Harassment or Intimidation: Employees shall not use the ALPR system to harass and/or intimidate any individual or group.
3. Use Based on a Protected Characteristic. Employees shall not use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
4. Personal Use: Employees shall not use the ALPR system or associated scan files or hot lists for any personal purpose.
5. First Amendment Rights. Employees shall not use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights. Anyone who engages in any prohibited use of the ALPR system or associated scan files, or hot lists may be subject to:
   a. criminal prosecution
   b. civil liability, and/or
   c. Administrative sanctions, up to and including termination

E. Staffing and Training

1. All patrol vehicles equipped with a dash camera will have the ALPR system enabled.
2. All employees using ALPR will be trained in this policy while they are training in the operations of their dash camera.

F. DME Collection

1. ALPR systems will be integrated into the RTCC for immediate investigative support.

2. ALPR captures license plates, vehicle attributes (make, color, visible damage or visual features), date, time, location, and camera/vehicle that captured the data.
3. ALPRs will only be used through dash camera mounted in patrol vehicles.
4. RTCC or any other employees assigned to ALPR operations shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute in any manner ALPR DME without prior authorization and approval of the Chief of Police or his/her designee.
5. All access to ALPR DME must be specifically authorized by the Chief of Police or his/her designee, and all access is to be audited to ensure that only authorized users are accessing the data for legitimate and authorized purposes.

G. <u>DME Retention</u>

1. All DME shall be handled in accordance with all applicable laws and existing Department policy on data and record retention. (Department policies: *Digital Evidence Collection 3.10.025* and *CJIS Disposal of Media 2.02.015*).
2. ALPR data will be stored for 14 days, after which it will be automatically purged unless directly tied to an active criminal investigation. Attaching ALPR data to a criminal case is an active process where purging the data is an automated function..

H. <u>DME Protection</u>

1. All data retained will be stored in a secure government digital evidence management system that include:
   a. FedRAMP Certification
   b. Encrypted Storage
   c. Robust Audit Trails
   d. Third-Party Validation
   e. Agency Controlled Access
2. All DME downloaded from a video management solution to a mobile workstation or to digital evidence storage like *Axon Evidence* shall be accessible only through a login/password protected system capable of documenting all access of information by name, date and time.
3. All data will be closely safeguarded and protected by both procedural and technological means.
4. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or Department-related civil or administrative action.

I. <u>DME Access & Sharing</u>

1. Citizen requests for digital evidence must be submitted in writing through the Department's *Public Records Request Portal* located on the Department's website.

2. Each request will be reviewed by Records Division for release eligibility and redaction requirements. Digital evidence will not be released if:

   a. It relates to an ongoing criminal investigation or prosecution

   b. It violates a court order

   c. It contains protected information

J. DME Privacy

1. Any access to collected DME will be logged and audited to ensure no unauthorized access has occurred.

2. Information gathered or collected, and records retained by the ALPR vendor cameras will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

K. Quarterly Review

On a quarterly basis, the Chief of Police shall assess ALPR operations and determine if the benefits ALPR provided to law enforcement and public safety outweigh the potential legal liability and risks to citizen privacy.

L. Audit Report

The Department will publish and annual report to include the following:

1. Number of hits

2. Number of arrests

3. Hits that are used for criminal investigations