



Automated License Plate Readers (ALPRs) for Parking Enforcement

Administrative
Regulation No. 7.02.002

1. **Overview of Purpose and Scope of this Regulation.**

The purpose of this Administrative Regulation regarding Automated License Plate Readers (ALPRs) for Parking Enforcement (which may be referred to herein as “ALPR Regulations”) is to provide guidance for capture, storage, and use of digital data obtained through the City’s use of ALPR technology for parking enforcement.

This policy applies to the use of ALPR technology by all City of Napa employees, officials, contractors and volunteers for parking enforcement purposes. This policy does not apply to NPD’s use of ALPR technology for law enforcement purposes. NPD’s use of ALPR technology for such purposes is governed by NPD Policy 431.

2. **Definitions.** The following definitions shall apply to this regulation:

“ALPR” means Automated License Plate Reader.

“ALPR Data” means license plate information such as license plate number, date, time, and location of where the scan was made.

“Hit” means a vehicle identified by the ALPR system as a vehicle parked beyond the allowed time in a timed parking space.

“Department” means the City of Napa Community Development Department.

“NPD” means the City of Napa Police Department.

“Parking Programs Manager” means the person designated by the Community Development Director to be responsible for managing City parking programs.

“Parking Enforcement Personnel” means the persons designated by the Community Development Director to be responsible for enforcing the City’s parking rules and regulations, including Napa Municipal Code Chapter 10.

“The Cloud” means any off-site server where data that belongs to the City is stored.

3. Administration.

3.1. The Parking Programs Manager is the official custodian of the City's parking enforcement ALPR system and is responsible for implementation of this policy. The Parking Programs Manager shall oversee the installation and maintenance of ALPR technology for the purpose of Parking Enforcement, as well as ALPR Data retention and access. The Parking Programs Manager will assign Parking Enforcement Personnel to administer day-to-day operation of the ALPR equipment and data. The job titles of Parking Enforcement Personnel are classified as Community Service Officer or Parking Ambassador.

4. ALPR Operation.

4.1. Parking Enforcement Personnel shall not use, or allow others to use, the ALPR equipment or database records for any unauthorized purpose.

4.1.1. Any ALPR owned and operated by the Department shall only be used for official Parking Enforcement business, including issuance, processing and appeals of parking citations.

4.2. No Parking Enforcement Personnel shall operate ALPR equipment or access ALPR Data without first receiving Department-approved training and access to the login/password-protected system from the Parking Programs Manager.

4.2.1. Training requirements include the following: understanding of City and State parking policies, ride-along with a trained Parking Ambassador using the ALPR system, and the passing of a performance assessment reviewed by a Parking Ambassador or the Parking Programs Manager.

5. ALPR Data capture and storage.

5.1. All ALPR Data uploaded to the Cloud shall be stored for a minimum of 2 years (Government Code § 34090) and in accordance with the City's Records Management Program Policy, currently documented in Resolution No. R2019-042. Thereafter, ALPR Data may be destroyed in accordance with the City's Records Management Program Policy.

5.2. The Parking Programs Manager is responsible for ensuring proper collection and retention of ALPR Data. Technical support shall be provided by the associated ALPR vendor to the Parking Programs Manager.

6. Accountability.

- 6.1.** All ALPR Data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time (Civil Code § 1798.90.52).
 - 6.1.1.** Parking Enforcement Personnel shall maintain a report of all ALPR Data accessed pursuant to this Policy. The report must include: (i) the username and organization/entity of the person accessing the ALPR Information, (ii) the date and time when the ALPR Data was accessed, (iii) the license plate number or other ALPR Data elements used to query the ALPR system, and (iv) the purpose for accessing the ALPR Data.
- 6.2.** ALPR audits should be conducted on a regular basis by the Parking Programs Manager or the authorized designee.
- 6.3.** Measures will be taken to ensure the accuracy of ALPR Data. Errors discovered in ALPR Data collected by ALPR units will be marked, corrected, or deleted in accordance with the type and severity of error in question.
 - 6.3.1.** When a read from the ALPR system registers as a Hit, the Parking Ambassador must compare the images of the original ALPR read and the most recent ALPR read. The Hit displays the following information for both the original and current reads: license plate number, a photo image of vehicle, date, time, and location. The Parking Ambassador must then confirm the read is the same vehicle, in the same original location, and has been parked beyond the allowable time. If the vehicle does not meet these criteria, it is considered a false Hit, and the record will then be corrected or deleted.

7. Data Security.

- 7.1.** Data collected by ALPR system shall be stored in a secured database facility. The secured database uses reasonable physical, technological, administrative procedural, and personnel security measures to prevent unauthorized access to ALPR Data. The Parking Programs Manager as the site manager has administrative control over access to the ALPR Data. The Parking Programs Manager shall have administrative user access to the ALPR database, as appropriate, to control:
 - 7.1.1.** The information to which a particular group or class of users can have access based on the group or class.
 - 7.1.2.** The information a class of users can access, and/or data being utilized in specific investigations.
 - 7.1.3.** Sharing capabilities with other law enforcement agencies.
 - 7.1.4.** Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the data or equipment.

- 7.1.5.** In the case of data breach/compromise of ALPR information owned or operated by the City, the following procedures are required:
- (i) For breaches within the City, if possible, Identify the breach/compromise and contact Vigilant support at support@vigilantsolutions.com or 925-398-2079. (ii) Pursuant to Civil Code 1798.29 and Civil Code, any victim of an ALPR data breach, will be notified and advised of the breach, and measures taken to fix the issue, without unreasonable delay.

8. Sharing of ALPR Data.

- 8.1.** City employees shall not sell, share, or transfer ALPR Data, except to another public agency, and only as otherwise permitted by law and this policy.

8.2. Law Enforcement Requests

- 8.2.1.** Napa PD may access ALPR Data for law enforcement purposes through login/password protected system capable of documenting all access of information by name, date, and time (Civil Code § 1798.90.52).

- 8.2.2.** ALPR Data may be released to NPD and other authorized and verified law enforcement officials and agencies in connection with an ongoing criminal investigation using the following procedures:

- a.** The agency makes a written request for the ALPR Data that includes:
 - i. The name of the agency.
 - ii. The name of the person requesting.
 - iii. The intended purpose of obtaining the information.
- b.** The request is reviewed by the Community Development Director or the authorized designee and approved before the request is fulfilled.
- c.** The approved request is retained on file.

- 8.2.3.** Aggregated ALPR Data not related to specific criminal investigations shall not be released to any local, state, or federal agency or entity without the express written consent of the City Manager.

8.3. Public Records Act Requests

- 8.3.1.** ALPR Data may be subject to disclosure under the California Public Records Act. The City will review requests for ALPR Data on a case-by-case basis to determine whether the requested information is exempt from disclosure or is legally required to be disclosed pursuant to the CPRA (or other applicable law) and will respond to such request in compliance with applicable law.