Oceanside Police Department
Automated License Plate Reader Usage and Privacy Policy

A. Purpose of Policy

The purpose of this policy is to outline the use of Automated License Plate Reader (ALPR), the retention and security of the data and the data storage system (ALPR system).

B. Automated License Plate Reader Overview

The Mobile ALPR systems are mounted on Oceanside Police Department Patrol vehicles. The technology of the cameras are designed to randomly capture images of vehicle license plates, convert the plate characters into a text file using optical character recognition technology. The text file is sent to a computer and compared against databases containing records of stolen or wanted vehicles as well as vehicles associated with AMBER alerts, missing persons or subjects who are wanted by law enforcement agencies. When a match is detected the officer is notified by an audible alert and a notification message appears on the mobile digital computer screen (MDT) in the vehicle.

ALPR data from the Oceanside Police Department is uploaded to an ALPR server and transferred to the regional ALPR server maintained by the Automated Regional Justice Information System (ARJIS). The data transfer from OPD to ARJIS is copied to the regional server in near real time. The functionality of the alert is dependent upon the data transfer from OPD

Officers using a vehicle with ALPR technology must take into account the potential lag time between the last update of data and the alert by the ALPR system when receiving a response from a stolen or wanted vehicle. Any alert received is considered informational and subsequent action should be based on the OPD Policy and Procedures. Visual confirmation of the subject plate is required before further action should be taken on the alert.

C. Authorized Purposes for Use of ALPR

Access to ALPR data is for official law enforcement purposes only. Primary use of the database is to assist with locating stolen or lost vehicles, license plates, and wanted or missing persons, by cross checking alert list downloaded by California Law Enforcement Telecommunication System (CLETS). Secondly, officers have the ability to query data to aid in the prosecution of crimes, ongoing criminal investigations, crime prevention and detection.

D. ALPR Administrators

The Administrative Services Division Captain shall oversee this Policy in compliance with Civil Code 1798.90.5 *et seq*. This includes, but is not limited to (Civil Code 1798.90.51; Civil Code 1798.90.53):

1. Implementing training on the use of the ALPR system and the safeguards to protect the ALPR system and information from unauthorized access;
2. Maintaining Training Records of all authorized users.

3. Monitoring, ensuring, and auditing that the security of the information is maintained, shared, and disseminated in a manner consistent with individuals' privacy and applicable laws.
4. Working with the Custodian of Records and the Chief Information Officer to ensure proper retention, security and destruction of ALPR data.
5. Ensuring this Policy is posted on the Oceanside Police Department Website.
6. Maintaining open dialogue with ARJIS in regards to the security and use of data access in compliance with Civil Code 1798.90.52.

E. Security of the ALPR System/Training

Field Operation Supervisors will ensure users receive department approved training for Officers authorized to use and access ALPR system (Civil Code 1798.90.51; Civil Code 1798.90.53).

Authorized Information Technology staff shall have the responsibility for managing the ALPR Server and infrastructure. The City of Oceanside uses a multi-factor authentication, encrypted communication, firewalls and other system auditing, and security measures to minimize the risks of unauthorized access to the system.

Physical access is limited to law enforcement staff and select IT staff that have completed background investigations to comply with the FBI CJIS Security Policy 5.3. All such staff are required to complete bi-annual recertification with a passing score of 70 or above.

F. Privacy

Use of the data is for official law enforcement purposes only and is governed by the CLETS Policies, Practices and Procedures (PPP), FBI CJIS Security Policy 5.3 and the CLETS Agreement signed by the Chief of Police for the Oceanside Police Department and the Attorney General designee from the California Department of Justice. The use of the system is restricted to members approved to access ALPR data and then only for a legitimate right to know or need to know purpose.

H. Access and Accountability

ALPR data can only be accessed via the ARJIS database – State, Federal, Regional Enterprise Retrieval System (SRFERS). Authorized users must have an active account in the ARJIS Security Center and are mandated to follow the procedures for complex passwords that must be changed every 90 days. Users must enter a reason for access to ALPR data prior to the query. System requirements are built in the ALPR system that requires the user to populate specific fields in order to access the ALPR data. All ALPR data queries are subject to audit and kept in audit logs in accordance with the procedures outlined by ARJIS.

I. Retention

ALPR data stored on the server will be retained for period of twelve months. The retention policy is consistent with ARJIS, most local law enforcement agencies in the San Diego County Region and the majority of the agencies in California who have implemented ALPR systems since January 2015.

The records will purge from the server automatically. If the ALPR data is relevant to a criminal investigation, it is the responsibility of the Detective investigating the incident to document the data and retain the record with the case file.

J. Releasing ALPR Data

ALPR data is confidential information and is not open to public review. Other law enforcement officers requesting ALPR data captured by a mobile ALPR from OPD who do not have access to ARJIS or COPLink must provide the following information by written request:

1. The name of the Agency on an official department letterhead
2. The name and title of the person requesting the data.
3. The purpose and need for the request *i.e.*, Case number, Field Interview, or Citation number

All such requests, and any releases pursuant thereto, shall be maintained for a minimum of three years.

K. Policy Revisions

Updates regarding this Policy will be completed as required by changes with applicable statutes or discontinued use of the ALPR system.