Automated License Plate Readers (ALPRs)

462.1 PURPOSE AND SCOPE
The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

462.2 POLICY
The policy of the Imperial Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

462.3 ADMINISTRATION
The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Imperial Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by a Captain designated by the Chief of Police. The Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

462.3.1 ALPR ADMINISTRATOR
The Department shall assign a Captain as the ALPR Administrator. The ALPR Administrator shall be charged with managing the ALPR program and will be responsible for the administration of the Department's ALPR program pursuant to the policies contained herein in strict conformance with the provisions of Division 3, Part 4, Title 1.82.23 of the California Civil Code.

462.4 AUTHORIZED USERS
Access to the ALPR system and associated database(s) is limited to sworn law enforcement officers, dispatchers, community service officers and analysts assisting the Imperial Police Department for purposes of criminal investigations and vendors who provide maintenance and service for the ALPR.

462.5 TRAINING REQUIREMENTS FOR AUTHORIZED USERS
Prior to accessing any portion of the ALPR system all employees authorized to access the ALPR system and database(s) shall receive training and instructions on the proper use of the database and authorized used of the system, along with a copy of this policy.

Automated License Plate Readers (ALPRs)

462.6 RECORD OF ACCESS

The ALPR Administrator shall establish an access log for the ALPR system and database(s). That log shall record the following information:

(a)   The identity of the authorized user that accessed the system and/or database(s);

(b)   The date and time that an authorized user accessed the system and/or database(s);

(c)   The license plate number or other data elements used to query the ALPR system; and

(d)   The purpose for accessing the system and/or database.

462.7 USERNAMES AND PASSWORDS

Each authorized user of the ALPR system shall be assigned a unique username and password. In order to access the system and/or database(s) all authorized users shall be required to use their username and password to log into the system.

462.7.1 SHARING OF USERNAMES AND PASSWORDS PROHIBITED

Authorized users shall not share their passwords with any person unless directed to do so by the ALPR Administrator or the Chief of Police.

Authorized users are responsible for safeguarding their passwords. If an authorized user believes that his or her password has been compromised it shall be the responsibility of the authorized user to change the password as soon as possible. It shall further be the responsibility of the authorized user to notify they ALPR Administrator immediately in the event the authorized user suspects that his or her password has been compromised.

Utilizing another authorized user's username and password is prohibited. Any City employee accessing the ALPR system and/or database(s) by using a username not assigned to that person may be subject to: criminal prosecution, civil liability, and/or administrative sanctions, including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

462.8 MONITORING COMPLIANCE

The ALPR Administrator shall be responsible to perform audits on the use of the ALPR system on a quarterly basis. The audits will be conducted to ensure users are in compliance with policy and the laws associated with the use and collection of ALPR data.

462.9 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Authorized users shall not use, or allow others to use the equipment or database records for any unauthorized purpose:

(a)   The ALPR system shall only be used for official law enforcement business.

Automated License Plate Readers (ALPRs)

(b)   The ALPR system may be used in conjunction with any routine patrol operation or criminal investigation.

(c)   Reasonable suspicion or probable cause is not required before using an ALPR.

particular consideration should be given to using ALPR-equipped cars to canvas areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(e)   No member of this department shall operate ALPR equipment or access ALPR data without first completing Department-approved training.

(f)   No member of this Department may access department, state or federal data unless otherwise authorized to do so.

(g)   If practicable, an ALPR response should be verified through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

462.10 PROHIBITED USES

The following uses of the ALPR system are specifically prohibited:

(a)   Invasion of Privacy. Except when done pursuant to a court order, 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).

(b)   Harassment or Intimidation. It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

(c)   Personal Use. It is a violation of this policy to use the ALPR system or associated scan files or hotlists for any personal purpose.

Anyone who engages in an impermissible use of the ALPR system or associated scan files or hotlists may be subject to: criminal prosecution, civil liablity, and/or administrative sanctions, including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

462.11 PUBLICATION OF THIS POLICY

Upon adoption by the City Council, a copy of this policy and any other policies or regulations pertaining to the City's ALPR program shall be available for inspection and copying by the general public. Further a true and correct copy of this policy and any other policies or regulations

DRAFT   Automated License Plate Readers (ALPRs) - 3

Automated License Plate Readers (ALPRs)

pertaining to the City's ALPR prgoram shall be conspicuously posted on the City of Imperial Police Department's website.

462.12 DATA COLLECTION AND RETENTION

The ALPR Administrator shall be responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the

All collected ALPR data remains the property of the Imperial Police Department. This data will not be sold, and will only be shared with other law enforcement agencies where the Imperial Police Department deems this sharing of information to be beneficial for improving public safety. The Imperial Police Department is solely responsible for determining those agencies with which it will share data, the length of the data sharing agreement, and establishing access to the data using a secure system that meets or exceeds the relevant aspects of the FBI-CJIS Security Policy.

All ALPR data downloaded to the server should be stored for a minimum of two years (Government Code § 34090) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

462.13 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The Imperial Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(a)   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).

(b)   Members 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 relate to a specific criminal investigation or [department/office]-related civil or administrative action.

(c)   ALPR system audits should be conducted on a regular basis.

For security or data breaches, see the Records Release and Maintenance Policy.

462.14 RELEASING ALPR DATA

ALPR data collected by the Imperial Police Department is considered law enforcement sensitive and will be used for official use only in accordance with the Driver's Privacy Protection Act (18 U.S. Code § 2721). The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, as outlined in a Memorandum of Understanding, or using the following procedures:

(a)   The agency makes a written request for the ALPR data that includes:The request is reviewd by the ALPR Administrator assigned to manage the ALPR program or the authorized designee and apporved before the request is fulfilled.

1.   The name of the agency.

2.   The name of the person requesting.

3.   The intended purpose of obtaining the information
   .

(b)   The request is reviewed by the ALPR Administrator assigned to manage the ALPR program or the authorized designee and approved before the request is fulfilled.

(c)   The apporved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

462.15 TRAINING
The Training Manager should ensure that authorized users receive department-approved training for those authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53).