City of San Jose, California

COUNCIL POLICY

TITLE Automated License Plate. Recognition for Parking Operations	**PAGE** 1 of 3	**POLICY NUMBER**
EFFECTIVE DATE January 1, 2019		**REVISED DATE** NA
APPROVED BY COUNCIL ACTION October 30, 2018 by Resolution No. 78846		

PURPOSE

The City of San Jose utilizes Automated License Plate Recognition (ALPR) technology to capture, analyze, and store digital license plate data and images to enable the rapid identification of vehicles in support of parking operations, compliance activities and public safety. In connection with its use of ALPR technology, the City recognizes established privacy and data breach notification rights of the public.

The purpose of this policy is to define the City's appropriate use, maintenance, collection, security, and retention of all ALPR Information, and the authorized users of the City's ALPR technology, in compliance with all applicable federal, state, and local laws.

DEFINITIONS

Automated License Plate Recognition System (ALPR): Means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of vehicle license plates and characters they contain into computer-readable data.

Automated License Plate Recognition end-user (ALPR end-user): Means a person who accesses or uses the ALPR system.

ALPR Information or ALPR Data: Means information or data collected through the use of the ALPR system.

ALPR Operator: Means a person or group with oversight responsibility for the ALPR system.

PARCS: Parking Access and Revenue Control System

AUTHORIZED USES

The use of ALPR systems and related data is restricted to the support of official City parking operations and enforcement activities, such as:

1. Serving as access control credentials for City owned and/or operated parking facilities
2. Parking revenue protection and fraud prevention
3. Auditing and accountability of parking transactions
4. Enforcement of parking rules, regulations, and restrictions

Additionally, as set forth in San Jose Police Department (SJPD) Duty Manual Addition L4207 – Use of ALPR Technology, ALPR may also be used by the City for legitimate law enforcement and public safety purposes.

RESTRICTED USES

The City will only use ALPR Technology to collect license plate data within public view. The City will not use ALPR Technology for the sole purpose of monitoring individual activities that are otherwise protected by the First Amendment to the United States Constitution.

The City will not share ALPR Information with any commercial or private entity, other than City parking contractors and enforcement vendors, as necessary for the conduct of City parking operations. Information gathered or collected and records retained by the City will not be:

1. Sold, published, exchanged or disclosed for commercial purposes

2. Disclosed or published without authorization

3. Disseminated to persons not otherwise authorized to access or use the ALPR Information

The City will not confirm the existence or nonexistence of ALPR Information to any person or agency who would not otherwise be eligible to receive the information under either this Policy or applicable law.

AUTHORIZED USERS

Authorized users with access to ALPR data shall include staff with a City operational need who specifically oversee and/or are responsible for parking operations and enforcement within City Departments including, Transportation, Parks, Airport, and Police as authorized by the respective department head, as well as City contracted parking operations and enforcement vendors.

TRAINING

Pursuant to California Civil Code Section 1798.90.51 (b), all Authorized Users shall receive training prior to being provided access to ALPR system and data. A record of all completed trainings will be maintained by the respective City departments. Training shall include:

1. Applicable federal and state law

2. Functionality of the equipment

3. Safeguarding password information, access to the ALPR systems, and ALPR Information.

ALPR DATA RETENTION

The City shall retain ALPR Data for the length of time established by each City department for official City use. Once the retention period has expired, the City will purge the record entirely from all active and backup systems.

ALPR DATA SECURITY

The City will closely safeguard all ALPR Data, and the City will monitor access to ALPR Data by procedural and technological means.

1. ALPR Data shall be accessible only through a login-password protected system capable of documenting all information accessed by username

2. All network equipment and servers containing sensitive data are maintained in a secured location and accessed only by authorized personnel

3. ALPR system shall maintain a log of successful and unsuccessful logon attempts, with such logs monitored by department Authorized Users

4. ALPR system workstations and servers shall be updated with latest security patches on a regular basis

5. ALPR Data shall be secured, encrypted and backed up regularly

6. ALPR Data shall reside on a firewall protected network

7. ALPR system notifications will be monitored and reviewed with action taken as necessary

DATA BREACH NOTIFICATION REQUIREMENTS

Following the discovery of a breach of the ALPR system that results in unauthorized third party disclosure of personal information, the City shall disclose the breach to all impacted individuals, in the most expedient time possible and without reasonable delay, by providing a notification to those reasonably believed to have been affected by the breach, and include the following:

1. Titled “Notification of Data Breach”
2. “What Happened”
3. “What Information Was Involved”
4. “What We Are Doing”
5. “What You Can Do”
6. “For More Information”
    a. Name and contact information for department reporting the breach
    b. A list of the personal information subject to the breach
    c. Either the date, estimated date, or the date range that the breach occurred if the information can be determined when the notice is provided
        i. If notification was delayed as a result of law enforcement investigation
        ii. A general description of the breach incident