RESOLUTION NO. 22-002

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SARATOGA ESTABLISHING A POLICY FOR AUTOMATED LICENSE PLATE READERS

WHEREAS, Automated License Plate Reader (ALPR) cameras are used by police departments across the United States to instantly capture license plate information and compare it against lists of license plates associated with stolen vehicles, people who have committed a crime, and for other investigative purposes; and

WHEREAS, many organizations that have used ALPR technology have found it to be an effective tool in fighting crime; and

WHEREAS, California Civil Code Section 1798.90.5 requires that public agencies with ALPRs adopt and implement a usage and privacy policy that identifies the individuals who will have access to the ALPR data, describes how the ALPR system will be monitored, lists parameters for sharing of ALPR data, describes measures that will be taken to protect the accuracy of ALPR data, and specifies the retention period for ALPR data.

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of Saratoga hereby adopts the attached Automated License Plate Reader Policy for the use of ALPR cameras in the City of Saratoga.

The above and foregoing resolution was passed and adopted at a regular meeting of the Saratoga City Council held on the 2nd day of February 2022 by the following vote:

AYES: COUNCIL MEMBERS BERNALD, KUMAR, ZHAO, VICE MAYOR FITZSIMMONS, MAYOR WALIA

NOES: NONE

ABSTAIN: NONE

ABSENT: NONE

Tina Walia.

Tina Walia, Mayor

ATTEST:

Britt Avrit, MMC, City Clerk

DATE: 2-9-2022

CITY OF SARATOGA AUTOMATED LICENSE PLATE READER POLICY
Adopted February 2, 2022 via Resolution 22-002

I. Purpose

The City of Saratoga ("City") leases an Automated License Plate Reader (ALPR) system within the City operated by the Santa Clara County Sheriff's Office ("Sheriff's Office") for certain law enforcement and public safety purposes. ALPR systems use high speed cameras to photograph vehicle license plates. The City intends to contract with vendors for installation and maintenance of the ALPR system. The City ALPR system may also obtain data from ALPR cameras not owned or leased by the City. This policy applies to data held within the City's ALPR system but does not apply to data held independently by the owners or lessors of ALPR cameras not owned or leased by the City. The City ALPR system is intended only to be used for authorized law enforcement and public safety purposes and its data are only intended to be access by authorized users.

California Civil Code section 1798.90.5 requires public agencies operating ALPR systems to adopt and implement a usage and privacy policy in order to ensure that the collection, use, maintenance, sharing, and dissemination of information collected pursuant to such system protects individual privacy and civil liberties. Consistent with the City's commitment to individual privacy and civil liberties and the State law mandate, the City has adopted this policy to regulate the use, management, retention, and other aspects of the City's ALPR system. This policy shall be made available to the public in writing and posted on the City website.

II. Authorized and Prohibited Uses

The City ALPR system shall only be utilized for the following purposes:

- To locate stolen, wanted, and/or other vehicles that are the subject of an investigation
- To locate and/or apprehend individuals subject to arrest warrants or who are otherwise lawfully sought by law enforcement
- To locate victims, witnesses, suspects, and others associated with a law enforcement investigation
- To locate missing persons, including in response to Amber Alerts and Silver Alerts
- To support local, State, Federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes
- To protect participants at special events; and
- To protect critical infrastructure sites.

Any data obtained from the City ALPR system shall be used and handled pursuant to this policy and applicable State and Federal law. All other uses not referenced above are prohibited. The ALPR system shall under no circumstances be used for personal or commercial purposes or any other purposes not specifically authorized above. Access to the ALPR system does not negate the need to comply with other laws or regulations including

the requirement to obtain a search warrant when legally required. The City shall at no time maintain an account for the ALPR system that allows the City to access the data collected or stored by the ALPR system.

III. Data Collection

Digital images of vehicle license plates and their associated license plate numbers shall be collected by the City ALPR system. The ALPR system shall collect the date and time that the license plate passes a digital-image site where an ALPR is located together with a captured vehicle's geographical location and vehicle details (make, model, type, and color). Live video, vehicle speeds, and audio shall not be provided or recorded. The ALPR system shall be designed, to the extent practicable, to blur images of individuals that may be inadvertently collected by the system.

IV. Data Access, Storage, and Protection

The City's ALPR system may only be used by, and data collected thereunder shall be accessible only by, personnel of the Sheriff's Office pursuant to a contract providing law enforcement services to the City. The City's ALPR system shall be accessible only through a login and password protected system capable of documenting individual user access by name, date, and time.

In addition to this policy, Sheriff's Office personnel shall observe and comply with the Sheriff's Office Surveillance Use Policy and any additional guidelines and regulations that are in place governing ALPR use and access. Prior to City's grant of use and access, the Sheriff's Office shall execute an agreement with the City and/or the City's contracted ALPR vendor(s), to the satisfaction of the City Attorney, agreeing to comply with this policy.

Contracts with vendors for the operation, maintenance, and repair of the ALPR system shall provide that the vendor is not authorized to access data collected by the ALPR system under any circumstances. Such vendors shall only be tasked with the operation, inspection, troubleshooting, and maintenance of the system hardware and software, associated cloud storage mechanisms and servers, as necessary.

Data collected by the City ALPR system is automatically uploaded to the ALPR system's associated cloud storage at the time of capture. Cloud storage and server capacity shall be provided for and maintained by the City's contracted ALPR vendor as part of the scope of services. The City shall confirm that the contracted vendor installs and implements appropriate security measures for such storage including encryption, firewalls, authentication, and other reasonable data protection measures.

Data stored in the City ALPR system cloud space shall not be downloaded to a local server, stored locally on a hard drive or portable device, or provided in a physical printout, except in the following cases:

- Where vehicle license plate image and numbers have been identified by the ALPR system as a match to a law enforcement registry
- Where data retrieval is necessary for conducting or assisting with a criminal investigation, or to facilitate an authorized use identified in Section II above

Only personnel from the Sheriff's Office working in an investigative or enforcement function may download ALPR data for local storage or printout (collectively, "Local Data") for authorized purposes stated herein. Data from the City ALPR system may not otherwise be downloaded for any other purpose, whether by Sheriff's Office authorized personnel or by City staff or other individuals or entities.

Local Data shall be maintained in accordance with applicable State and Federal evidentiary laws and in accordance with appropriate chain of custody practices. Additionally, the Sheriff's Office shall implement physical security, encryption, firewalls, authentication, and other reasonable security measures to protect Local Data that it has retrieved from the system.

Local Data shall be accessible only through a login and password protected system capable of documenting individual user access by name, date, and time.

V. Data Retention

Data stored in the ALPR cloud system shall be purged after thirty (30) days from the date it was uploaded to the cloud system unless downloaded or stored pursuant to Section IV above.

Data that is downloaded or stored pursuant to Section IV above shall be purged no later than six (6) months from the date it was downloaded for local storage, unless the data thereafter becomes associated with a criminal investigation or an ongoing case for an authorized purpose identified in Section II above. In the latter case, the data shall be retained for the duration of the criminal investigation and the criminal proceedings through adjudication of the case in the same manner as other evidence in the matter, unless otherwise ordered by the court to be retained for a longer period or permanently.

VI. Public Access

Data from the City ALPR system shall not be sold, shared, or transferred except as specifically authorized by this policy. Data from the City ALPR system shall not be made public, unless specifically required by State of federal law, or by court order. If a public request for data is received, the Sheriff's Office shall consult with the Santa Clara County Counsel's Office to determine whether the requested data is exempt from disclosure pursuant to the California Public Records Act or other State of Federal law provisions, and whether any additional steps are required in response to such a request for data.

VII. Third-Party Data Sharing

Data-sharing from the City's ALPR system shall be limited to only the following:

- District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence
- Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with California criminal discovery laws; and
- Other law enforcement offices as part of a specific formal criminal or administrative investigation
- Parties to civil litigation, in response to a court order.

VIII. Training

All personnel authorized to use and access the ALPR system and data pursuant to this policy shall receive all required training from the Sheriff's Office. Said personnel shall also review and receive copies of this policy and the Sheriff's Office Surveillance Use Policy.

IX. Oversight

The Sheriff's Office shall ensure compliance with this policy as the provider of law enforcement services to the City.

All access to ALPR system data shall be logged, and the Sheriff's Office shall maintain an audit trail of requested and accessed information, including the purpose of the search. Periodic, random audits shall be conducted by the Sheriff's Office and on at least an annual basis. Audits shall ensure compliance with this policy and all applicable laws, and shall be used to ensure the accuracy of ALPR information and correct data errors. Audit reports shall contain at least the following information:

- Name of law enforcement agency that accessed the data
- Date and time of access
- Reason for accessing data
- Activity executed, including any license plate numbers searched identified in a separate confidential appendix
- Incident number associated with the investigation

Upon completion of each audit, the Sheriff's Office shall provide a copy of the audit report to the City Manager or the City Manager's designee within five (5) business days of completion.