STAFF REPORT

City Council
Meeting Date: **10/8/2024**
Staff Report Number: **24-179-CC**

Regular Business: **Authorize the city manager to execute an agreement with Flock for fixed Automated License Plate Readers and waive the first reading and introduce an ordinance amending Menlo Park Municipal Code Chapter 2.56 "Public Safety Information"**

Recommendation

Staff recommends the City Council authorize the city manager to execute a master services agreement (MSA) with Flock Safety (Flock) to implement and operate fixed automated license plate readers (ALPRs), and waive the first reading and introduce an ordinance amending Menlo Park Municipal Code Chapter 2.56 "Public Safety Information."

Policy Issues

ALPR technology receives guidelines and governance from state and local law, and from agency policy.

California Civil Code requires that any public agency provide an opportunity for public comment at a regularly scheduled public meeting before implementation of an ALPR program. The statutory Civil Code requirement has been met, most recently during City Council meetings in September 2023 and May 2024.

Menlo Park Municipal Code Chapter 2.56 regulates the process of collecting, utilizing, and retaining public safety data such as the type of data collected by ALPRs. This Municipal Code section was established in conjunction with the City's original ALPR deployment in 2014. Before deployment of the proposed fixed ALPRs, revisions must be made in the Municipal Code to ensure it applies properly to both mobile (mounted to vehicles) and fixed (to be provided by Flock) ALPRs, and the data collected by both systems. An ordinance to update Chapter 2.56 is available in Attachment A. A red-line version of changes to Chapter 2.56 is available in Attachment B.

The Menlo Park Police Department (MPPD) also has a comprehensive Lexipol policy governing ALPRs (Policy 462), which provides strict guidelines for administration, operation, data collection and retention, accountability and training, as well as auditing and reporting (as in the MPPD quarterly report). This Lexipol policy has also been updated to ensure recognition of the community's needs and the adjustments to operations in relation to fixed license plate readers and the revised Municipal Code (Attachment C).

Background

The City Council held a study session Sept. 26, 2023, on Flock fixed ALPRs and gunshot detection technology. Over the two-and-a-half-hour study session, the MPPD presented and the City Council received public comment, with the following summary:

- An overview of ALPR Technology and its history deployed with MPPD on three patrol vehicles dating

back 10 years.
- An overview of the City's Municipal Code governing data from ALPR technology, also dating back to 2013, and the rigor of this City's retention policy by ordinance (six months compared to typical one year).
- An explanation of the capabilities and use of Flock equipment and operating systems, and an explanation of how data moves through Flock, but is completely owned, controlled, and retained by the City and MPPD.
- An explanation of the retention of the data, law, security and controls in place – both currently and the future of this should fixed ALPRs be deployed.
- An illustration of means of police access to the data, and the policy, security and controls in place, with a view of the future should fixed ALPRs be deployed. Sharing agreements between police agencies were also discussed.
- A discussion on the reasons for seeking Flock as the vendor, based on the capabilities and the robust deployment of Flock technology throughout San Mateo County and other nearby jurisdictions.
- An overview of the transparency webpages set up by many agencies using Flock technology and MPPD's commitment to follow a similar path.
- A summary of numerous very recent and hyper-local examples of the application of this data used to stop and solve crime, locate people at risk, and enhance the safety of the public through the prevention of future crimes and disorder.
- A description of the initial and revolving costs for implementation of this technology.

The City Council indicated a need for additional information including comparative information to alternatives, the relationship of crime data to the implementation of fixed ALPR in other jurisdictions, more information about the security and accountability of these systems, and specifics on policy and City ordinance changes needed to include commitments on agency sharing, transparency of use and accountability to the community.

In February, the City Council received additional public comment regarding ALPRs from community members. At the regular City Council meeting March 12, the City Council discussed the item and directed staff to re-agendize the discussion of fixed ALPRs at a future meeting including the following information:.
- A revised look at costs for implementations, to include scaling options and a comparison to alternatives.
- An exploration of the relationship of crime numbers to implementation of fixed ALPRs in other jurisdictions, and an explanation of how this technology is effective in relation to public safety.
- Discussion on the retention, access, and security control of this technology.
- A review of revisions needed to MPPD policy and the City's ordinance governing the collection and use of ALPR data.

On May 7, the City Council held a study session on ALPRs. Through dialogue with City Council and additional public commentary, the City Council directed staff to include Flock fixed ALPRs in the fiscal year 2024-25 budget, with recommendations for modifications to the Municipal Code and MPPD policy. Note: the fiscal year 2024-25 budget was adopted June 25 and included the implementation of Flock fixed ALPRs.

As part of the staff presentation and follow-up discussion May 7, staff provided multiple references to City Council regarding research completed in staff's quest to provide a proposal that met interests based on concerns brought up in public discussion. This included advisory work completed by the American Civil Liberties Union, New York University's Policing Project, various academic papers, and reference policy and ordinance material from the Town of Los Altos, which engaged closely with American Civil Liberties Union (ACLU) in their process before implementation in 2023. All of this information was in consideration and

utilized during the planning and preparation of the current request herein.

Analysis

The MSA that governs the business relationship between Flock and the City in relation to the implementation and utilization of fixed ALPRs is available in Attachment D. Staff has worked with the vendor (Flock) and the city attorney's office to negotiate a MSA that meets the interests and needs of both parties (City of Menlo Park and Flock). Additionally, an invoice from Flock that enumerates implementation and operation costs for the next two years is available in Attachment E. As this expense, while anticipated and authorized in the budget, is above the city manager's signing authority, staff is requesting City Council authorize the city manager to execute the MSA.

The MSA refers to three exhibits; an "order form" (which will follow the details of the attached invoice), a proof of insurance, which is always required for such business relationships, and a customer implementation guide, which will govern the operational aspects of implementation. All of these items will be added at the time of the execution of the agreement.

To re-emphasize previous commitments to process – Flock implements the hardware technology and provides the software and database for data collected. The data collected through the Flock system is owned and controlled entirely by the City of Menlo Park and not Flock. As stated in §4.2 of the MSA: "Flock does not own and shall not sell Customer Generated Data."

Staff has also worked with the city attorney's office to refresh the city's Municipal Code Chapter 2.56 to reflect the use of data obtained by the City through Flock ALPR technology, provide some reassurances to our public regarding ethical and legal use of this technology, and reduce the retention of data per City Council request from six months down to 30 days. Staff feels that the Municipal Code is appropriately revised and ready for final review and approval by City Council (Attachment A).

<u>Overview of changes - Menlo Park Municipal Ordinance Chapter 2.56 et seq.</u>

- Modification of terms in sections referring to the transfer of data, retention, and access to information to reflect the addition of the Flock asset.
- Referral of access to agencies engaged for "sharing" through the Flock Database – this will require written acknowledgement from both agencies and an agreement that the data is used "for legitimate law enforcement purposes and by authorized/trained personnel and only in compliance with all policies, procedures and reporting requirements of Menlo Park PD and its written agreement with Flock Safety."
- A section under "Prohibited Use" (§2.56.040) committing that Menlo Park does not permit the sharing of ALPR data gathered by the City, vendors or subcontractors, as defined below, for:
  1. Any purpose that violates this policy or any applicable laws and regulations;
  2. The purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code §7282.5: Government Code §7284.2 et seq) - these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP); or
  3. Any purpose that would assist another state to carry out enforcement actions that violate California laws.
- Continued commitment to MPPD's quarterly reporting reiterated in the ordinance, with the addition of Flock data to quarterly reports.

Staff has also revised departmental policy (Attachment C) to align with the new technology, as well as the ethical and legal provisions outlined in the revised Municipal Code. Additionally the revised department

policy outlines strict requirements for training of all personnel using the system, an appropriate outside auditing process, and a renewed and policy-articulated commitment to production of accountability-related data in the MPPD quarterly report to City Council.

Overview of changes – MPPD Policy 462 – ALPRs

- The "Purpose and Scope" section (462.1) of the policy was updated to reflect following priorities, among others:
  - Minimizing threat and risk of injury to individuals.
  - Promoting governmental legitimacy and accountability.
  - Minimizing potential risks to individual privacy, civil rights and civil liberties.
  - Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
  - Increasing trust by maximizing transparency.
- A "Policy" section (462.2) has been added that lays out the general mission in regard to ALPR. In this section, there is added language consistent with the Municipal Code changes in regard to compliance with certain specific laws, and our commitment not to assist through information sharing in actions that go against California law:
  1. Any purpose that violates this policy or any applicable laws and regulations;
  2. The purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code §7282.5: Government Code §7284.2 et seq) - these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP); or
  3. Any purpose that would assist another state to carry out enforcement actions that violate California laws.
- The "Operations" section (462.4) of the policy was amended substantially, since the previous iteration of MPPD ALPR technology was far less interactive:
  - Emphasizing requirements of acknowledgement of the policy and required training
  - Access control instructions (use of individual accounts, and log in / out) receives more detail and requirements.
  - Explicit requirements to verify any system "alerts" absent exigent circumstances involving immediate safety needs – "Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated or unless exigent circumstances exist."
  - A highly expanded and very detailed section instructing officers on requirements involving "hot lists" - both identifying requirements for constant refreshing of the lists to minimize "false positives," and laying our strict guidelines for any agency entries to the "hot list." This includes highly accountable documentation for entries, and distinct documentation for "hot list" stops.
- A distinct "Permitted/Prohibited Uses" section (462.4.1) was added, specifically calling out certain prohibitions:
  - Invasion of Privacy (limiting use only to vehicle license plates viewable from a public area).
  - Harassment or intimidation.
  - Any use solely based on a protected characteristic.
  - Any personal (non-police business) use.
  - Infringement upon First Amendment rights.
  - This section of the policy specifically reminds members that transgression of such prohibitions opens them up to potential criminal and civil liability, as well as discipline by this department.
- The "Data Collection and Retention" section (462.5) now matches the Policy to the revised Municipal Code.

  - It also includes a section committing that “Information gathered or collected, and records retained by Contracted Entities (i.e., Flock, for use of their database) will not be sold, accessed, or used for any reason other than legitimate law enforcement or public safety purposes. In accordance with this policy, data collected by ALPR cameras will not be accessed by Contracted Entities without prior authorization by the Chief of Police or his/her designee.”
  - Additionally, this section of the policy demands that purged data is completely “sanitized” and not retrievable.
- The “Accountability and Safeguards” section (462.6) contains detailed requirements for use of the data and access and will modify documentation and audit requirements to fit the new practices related to the Flock Database.
  - This section also notifies members that there is a distinct section of the policy in compliance with federal, state and local requirements that details security of data, requests and maintenance of this information (MPPD Policy 808 – Records Maintenance and Release).
- The “Releasing ALPR Data” section (462.7) lays out legal requirements for data requests per law, and the “Training” section (462.8) specifically requires that officers receive training before use of these systems. These are relatively unchanged.
- The “Auditing and Reporting” section (462.9) is modified to distinctly describe MPPD’s quarterly reporting requirement for ALPR-related information, and the establishment of a Transparency Portal accessible through the MPPD website.
- Staff added – “Contracted Entities” (462.10) to describe our relationship and expectations with Flock Safety, and “ALPR Locations” (462.11) to reinforce our mission to deploy fixed ALPRs equitably across our jurisdiction.

Impact on City Resources

First year costs associated with the MSA are already included in the adopted fiscal year 2024-25 budget and are summarized in Table 1 below. First year costs are $133,000 and ongoing annual costs will be $112,500. For a reference point, this annual cost is approximately equal to half the fiscal impact of one sworn employee of the MPPD .

The MPPD will use available funds through the State Supplemental Local Law Enforcement Grant (SLESF) to cover a portion of year one implementation expenses of $20,500. Sufficient reserves from previous SLESF awards exist to cover this expense.

The police and public works departments are also assessing the traffic analytics function available through these fixed ALPR cameras to provide data on traffic flow and frequency. If determined to be useful, implementation of traffic analytics could be covered within existing departmental budgets ($500.00 per camera per year, where helpful).

Table 1: Flock project costs	
Item	**Cost**
Flock Falcon ALPR cameras (35 at about $3000 ea.)	$105,000
Flock advanced search operating system	(Annual) $7,500
Total ongoing – cameras, software and secure data storage	**$112,500**
Professional services implementation fees (first year only – paid through SLESF)	$20,500
Total first year	**$133,000**
Total second year	**$112,500**
Two (2) year total	**$245,500**

Environmental Review

This action is not a project within the meaning of the California Environmental Quality Act (CEQA) Guidelines §§15378 and 15061(b)(3) as it will not result in any direct or indirect physical change in the environment.

Public Notice

Public notification was achieved by posting the agenda, with the agenda items being listed, at least 72 hours prior to the meeting.

Attachments

A. Ordinance authorizing modification of Menlo Park Municipal Code Chapter 2.56
   Exhibit A – Chapter 2.56 text
B. Menlo Park Municipal Code Chapter 2.56 – redline of changes
C. Menlo Park MPPD Lexipol Policy 462
D. MSA – City of Menlo Park and Flock Safety
E. Invoice from Flock Safety

Report prepared by:
Dave Norris, Police Chief

Report reviewed by:
Justin Murphy, City Manager
Stephen Stolte, Assistant City Manager

ORDINANCE NO. XXXX

ORDINANCE OF THE CITY COUNCIL OF THE CITY OF MENLO PARK AMENDING MENLO PARK MUNICIPAL CODE CHAPTER 2.56 TO UPDATE THE CITY'S AUTOMATED LICENSE PLATE READER REGULATIONS

WHEREAS, the City of Menlo Park is a general law city; and

WHEREAS, automated license plate reader ("ALPR") technology allows for the automated detection of license plates from mobile and fixed ALPR cameras; and

WHEREAS, on June 3, 2014, the City Council adopted Ordinance No. 1007 and enacted Chapter 2.56 of the Menlo Park Municipal Code to regulate the use of ALPR technology in the City; and

WHEREAS, on Oct. 5, 2017, the Governor signed the California Values Act (Senate Bill 54) into law; and

WHEREAS, the California Values Act prevents state and local resources from being used to assist federal immigration enforcements; and

WHEREAS, since the City Council adopted Ordinance No. 1007, new best practices have emerged for the use of ALPR technology; and

WHEREAS, the City Council desires to update the Menlo Park Municipal Code to reflect developments in state law and best practices.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF MENLO PARK DO ORDAIN AS FOLLOWS:

Section 1. Findings.
The City Council of the City of Menlo Park does hereby find that the above referenced recitals are true and correct and material to the adoption of this ordinance.

Section 2. Amendment of Code.
Chapter 2.56 is hereby amended to read as set forth in the attached Exhibit A.

Section 3. Severability.
If any section, subsection, sentence, clause or phrase or word of this ordinance is for any reason held to be unconstitutional, unlawful, or otherwise invalid by a court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this ordinance.

Section 4. Effective date.
This ordinance shall take effect thirty (30) days after passage by the City Council. Increases in compensation shall take effect upon commencement of a new term of office by any City Councilmember.

Section 5. Publication
The City Clerk is directed to publish this Ordinance as required by State law.

//

INTRODUCED on the eighth day of October, 2024.

PASSED AND ADOPTED as an ordinance of the City of Menlo Park at a regular meeting of said City Council on the __ day of __, 2024, by the following votes:

AYES:

NOES:

ABSENT:

ABSTAIN:

APPROVED:

_____
Cecilia Taylor, Mayor

ATTEST:

_____
Judi A. Herren, City Clerk

Exhibits
A. Chapter 2.56

Chapter 2.56
PUBLIC SAFETY INFORMATION

Sections:

2.56.010 Purpose.

2.56.020 Definitions.

2.56.030 Automated license plate reader information use.

2.56.040 Prohibited use of automated license plate reader and automated license plate reader information.

2.56.050 Automated license plate reader auditing and reporting.

2.56.060 Public safety camera system data use.

2.56.070 Prohibited use of public safety camera system and data.

2.56.080 Public safety camera system auditing and reporting.

2.56.090 Adoption of department policies.

2.56.010 Purpose.

The purpose of this chapter is to provide for the proper use of data and recordings gathered by the city through the use of automated license plate reader system and the public safety camera system.

2.56.020 Definitions.

For the purposes of this chapter, the following words and phrases shall have the meanings ascribed to them in this section:

(1) “Automated license plate reader system” or “ALPR system” means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and covert images of registration plates and the characters they contain into computer-readable data.

(2) “Automated license plate reader information” or “ALPR information” means information or data gathered through the use of an ALPR system.

(3) “Public safety camera system” means cameras that record images only and not sound and that are placed in strategic fixed locations within the city at the direction of the chief of police and with the approval of the city council for the purpose of detecting and deterring crime, to help emergency services personnel maintain public order, to help manage emergency response situations during natural and manmade disasters, to monitor pedestrian and vehicle traffic activity, to assist in the preparation of traffic reports, and to assist city officials in prosecuting and/or defending civil or administrative actions.

(4) “Recordings” means the recorded images, without sound, recorded by the public safety camera system.

2.56.030 Automated license plate reader information use.

(a) ALPR information may be securely transmitted to an entity that is a part of a multi-jurisdictional public safety program created to assist local, state, federal and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and

dissemination of criminal threat information, including, but not limited to the Northern California Regional Intelligence Center (“NCRIC”), provided such entities have executed agreements with the city agreeing to comply with the retention/destruction provisions set forth in this section.

(b) ALPR information transmitted under this section from the police department shall be kept no more than thirty (30) days, and then destroyed, unless retention of ALPR information is necessary for an active criminal case or pursuant to a valid court order.

(c) ALPR information may only be accessed by law enforcement personnel who are approved to access the data and who have undergone required training for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related civil or administrative action.

(d) ALPR information may be accessed by other NCRIC agencies that have executed a memorandum of understanding with NCRIC, but only for legitimate law enforcement purposes and by authorized/trained personnel and only in compliance with all policies, procedures and reporting requirements of NCRIC.

(e) ALPR information may be released to other non-NCRIC authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, with approval of the chief of police or police commander, provided any such official and/or agency has executed an agreement with the city agreeing to comply with the terms and provisions of §§2.56.030 and 2.56.040.

(f) All data and images gathered are for official use of the police department and because such data may contain confidential California Law Enforcement Telecommunications Systems ("CLETS") information, it is not open to public view or inspection.

2.56.040 Prohibited use of automated license plate reader and automated license plate reader information.

(a) ALPR information shall not be used to invade the privacy of individuals, to look into private areas or areas where the reasonable expectation of privacy exists, nor shall they be used to harass, intimidate or discriminate against any individual or group, nor for any purpose not specifically authorized by this chapter.

(b) ALPR information shall not be used for any of the following:
  (1) any purpose that violates this policy or any applicable laws and regulations;
  (2) the purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code §7282.5: Government Code §7284.2 et seq) - these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP); or
  (3) any purpose that would assist another state to carry out enforcement actions that violate state or local laws.

(c) Unauthorized access, possession or release of data is a violation of police department policy and various federal and state criminal statutes. Any employee, who accesses, possesses or releases data, from the ALPR system without authorization or in violation of this chapter and such additional policies established by the police department, may face department discipline up to and including termination, criminal prosecution and/or civil liability.

2.56.050 Automated license plate reader system auditing and reporting.

(a) The police department will generate a report which shall indicate the number of license plates captured by the ALPR system in the city of Menlo Park, how many of those license plates were “hits” (on an active wanted list), the number of inquiries made by Menlo Park personnel along with the justifications for those inquiries, and information on any data

retained beyond thirty (30) days and the reasons for such retention in compliance with §2.56.030(b).

(b) Following generation and review of the quarterly ALPR report, described in subsection (a) of this section, the police department shall provide an information report to the city council.

(c) ALPR system audits will be randomly conducted by the California Department of Justice and in conjunction with yearly CLETS audits.

2.56.060 Public safety camera system data use.

(a) Public safety camera recordings may only be used for the purpose of criminal investigations, detecting and deterring crime, to help emergency services personnel maintain public order, to help manage emergency response situations during natural and manmade disasters, to monitor pedestrian and vehicle traffic activity, to assist in the preparation of traffic accident reports, and to assist city officials in prosecuting and/or defending civil or administrative actions.

(b) Recordings will be made in a professional, ethical and legal manner.

(c) All recordings will be stored by the police department in a secure location with access restricted to authorized persons, and shall not be accessible by third parties without express permission.

(d) Recordings not otherwise needed for reasons in subsection (a) of this section shall be retained for a period of no more than ninety (90) days and then erased or recorded over as limited by the storage capacity of the cameras.

(e) Any recordings needed as evidence in a criminal or civil case proceeding or for another reason specified in subsection (a) of this section shall be collected and booked in accordance with current police department evidence procedures.

(f) Recordings may only be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes as specified in subsection (a) of this section with approval of the chief of police or police commander, provided such official or agency executes an agreement with the city agreeing to comply with the terms and provisions of §§2.56.060 and 2.56.070, or with a valid court order.

(g) Except as required by a valid court order or other lawful process, recordings do not constitute public records and will not be disclosed to the public.

(h) Facial recognition and cognitive security software may only be used to review recordings from the public safety camera system with the approval of the chief of police or police commander in specific criminal investigations or specific threats to public safety.

2.56.070 Prohibited use of public safety camera system and data.

The public safety camera system will not be used to invade the privacy of individuals, to look into private areas or areas where the reasonable expectation of privacy exists. The public safety camera system shall not be used to harass, intimidate or discriminate against any individual or group, nor for any purpose not authorized by this chapter.

2.56.080 Public safety camera system auditing and reporting.

The chief of police or his/her designee will conduct an annual review of the public safety camera system, its use, effectiveness and adherence to policy, including frequency and purpose for use of facial recognition or cognitive security software and frequency and purpose for retention of recordings beyond ninety (90) days, and will provide an annual information report to the city council regarding such review.

2.56.090 Adoption of department policies.

The police department is directed to adopt policies to be included in its policy manual consistent with the provisions of this chapter, which policies may be more restrictive, but not less restrictive, than the policies set forth in this chapter.

Chapter 2.56

PUBLIC SAFETY INFORMATION

Sections:

2.56.010 Purpose.
2.56.020 Definitions.
2.56.030 Automated license plate reader ~~data~~ information use.
2.56.040 Prohibited use of automated license plate reader and ~~data~~automated license plate reader information.
2.56.050 Automated license plate reader auditing and reporting.
2.56.060 Public safety camera system data use.
2.56.070 Prohibited use of public safety camera system and data.
2.56.080 Public safety camera system auditing and reporting.
2.56.090 Adoption of department policies.

2.56.010 Purpose.

The purpose of this chapter is to provide for the proper use of data and recordings gathered by the city through the use of automated license plate reader systems~~,~~ and the public safety camera system. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.020 Definitions.

For the purposes of this chapter, the following words and phrases shall have the meanings ascribed to them in this section:

(1) "~~"~~Automated license plate reader system~~"~~" or "~~"~~ALPR system~~"~~" means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and covert images of registration plates and the characters they contain into computer-readable data~~technology, also known as license plate recognition, which provides automated detection of license plates~~.

(2) "~~"~~Automated license plate reader information" or "ALPR information~~Data~~~~"~~" means information or data gathered through the use of an ALPR system. ~~by the automated license plate reader in the form of license plates and metadata (location and time license plate was viewed).~~

(3) "~~"~~Public safety camera system~~"~~" means cameras that record images only and not sound and that are placed in strategic fixed locations within the city at the direction of the chief of police and with the approval of the city council for the purpose of detecting and deterring crime, to help emergency services personnel maintain public order, to help manage emergency response situations during natural and manmade disasters, to monitor pedestrian and vehicle traffic activity, to assist in the preparation of traffic reports, and to assist city officials in prosecuting and/or defending civil or administrative actions.

(4) "~~"~~Recordings~~"~~" means the recorded images, without sound, recorded by the public safety camera system. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.030 Automated license plate reader ~~data~~ information use.

(a) ALPR information~~Data~~ ~~will~~ may be securely transmitted to an entity that is a ~~the Northern California Regional Intelligence Center ("NCRIC") or to the Flock Database as~~ part of a multi-jurisdictional public safety program created to assist local, state, federal and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and dissemination of criminal threat information, including, but not limited to the Northern California Regional Intelligence Center ("NCRIC"), provided ~~NCRIC and Flock Safety have~~such entities have executed agreements with the city agreeing to comply with the retention/destruction provisions set forth in this section.

(b) ~~Data~~ ALPR information transmitted ~~to NCRIC or to the Flock Database~~under this section from the police department shall be kept no more than ~~six (6) months in the case of NCRIC and no more than~~ thirty (30) days, and then destroyed, unless retention of ~~specific identified license plate data~~ALPR information is necessary for an active criminal case or pursuant to a valid court order.

(c) ~~Data~~ ALPR information may only be accessed by law enforcement personnel who are approved to access the data and who have undergone required ~~NCRIC or Flock Database~~ training for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related civil or administrative action.

(d) ~~Data~~ ALPR information may be accessed by other NCRIC agencies that have executed a memorandum of understanding with NCRIC, but only for legitimate law enforcement purposes and by authorized/trained personnel and only in compliance with all policies, procedures and reporting requirements of NCRIC.

(e) ~~Data~~ ALPR information may be released to other non-NCRIC authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, with approval of the chief of police or police commander, provided any such official and/or agency has executed an agreement with the city agreeing to comply with the terms and provisions of Sections 2.56.030 and 2.56.040.

(f) All data and images gathered are for official use of the police department and because such data may contain confidential California Law Enforcement Telecommunications Systems ("CLETS") information, it is not open to public view or inspection. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.040 Prohibited use of automated license plate reader and ~~data~~automated license plate reader information.

(a) ALPR information shall not be used to invade the privacy of individuals, to look into private areas or areas where the reasonable expectation of privacy exists, nor shall they be used to harass, intimidate or discriminate against any individual or group, nor for any purpose not specifically authorized by this chapter.

(b~~!!~~) ALPR information shall not be used for any of the following:~~The City of Menlo Park (including Menlo Park Police Department) does not permit the sharing of ALPR data gathered by the City, vendors or subcontractors, as defined below, for~~

(1) any purpose that violates this policy or any applicable laws and regulations;

(2) the purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code 7282.5: Government Code 7284.2 et seq) - these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP); or

(3) any purpose that would assist another state to carry out enforcement actions that violate state or local laws.

(c~~b~~) Unauthorized access, possession or release of data is a violation of police department policy and various federal and state criminal statutes. Any employee, who accesses, possesses or releases data, from the ALPR system ~~database~~ without authorization or in violation of this chapter and such additional policies established by the police department, may face department discipline up to and including termination, criminal prosecution and/or civil liability. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.050 Automated license plate reader system auditing and reporting.

(a) The police department will generate a report which shall indicate the number of license plates captured by the ALPR system in the city of Menlo Park, how many of those license plates were "hits" (on an active wanted list), the number of inquiries made by Menlo Park personnel along with the justifications for those inquiries, and information on any data retained beyond thirty (30) days, and the reasons for such retention in compliance with Section 2.56.030(b). ~~NCRIC will give a quarterly report to the police department which shall indicate the number of license plates captured by the ALPR system in the city of Menlo Park, how many of those license plates were ""hits"" (on an active wanted list), the number of inquiries made by Menlo Park personnel along with the justifications for those inquiries, and information on any data retained beyond six (6) months and the reasons for such retention in compliance with Section 2.56.030(b).~~

(b) Following generation and review of the quarterly ALPR report , described in subsection (a) of this section, the police department shall provide an information report to the city council.

(de) ALPR system audits will be randomly conducted by the California Department of Justice and in conjunction with yearly CLETS audits. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.060 Public safety camera system data use.

(a) Public safety camera recordings may only be used for the purpose of criminal investigations, detecting and deterring crime, to help emergency services personnel maintain public order, to help manage emergency response situations during natural and manmade disasters, to monitor pedestrian and vehicle traffic activity, to assist in the preparation of traffic accident reports, and to assist city officials in prosecuting and/or defending civil or administrative actions.

(b) Recordings will be made in a professional, ethical and legal manner.

(c) All recordings will be stored by the police department in a secure location with access restricted to authorized persons, and shall not be accessible by third parties without express permission.

(d) Recordings not otherwise needed for reasons in subsection (a) of this section shall be retained for a period of no more than ninety (90) days and then erased or recorded over as limited by the storage capacity of the cameras.

(e) Any recordings needed as evidence in a criminal or civil case proceeding or for another reason specified in subsection (a) of this section shall be collected and booked in accordance with current police department evidence procedures.

(f) Recordings may only be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes as specified in subsection (a) of this section with approval of the chief of police or police commander, provided such official or agency executes an agreement with the city agreeing to comply with the terms and provisions of Sections 2.56.060 and 2.56.070, or with a valid court order.

(g) Except as required by a valid court order or other lawful process, recordings do not constitute public records and will not be disclosed to the public.

(h) Facial recognition and cognitive security software may only be used to review recordings from the public safety camera system with the approval of the chief of police or police commander in specific criminal investigations or specific threats to public safety. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.070 Prohibited use of public safety camera system and data.

The public safety camera system will not be used to invade the privacy of individuals, to look into private areas or areas where the reasonable expectation of privacy exists. The public safety camera system shall not be used to harass, intimidate or discriminate against any individual or group, nor for any purpose not authorized by this chapter. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.080 Public safety camera system auditing and reporting.

The chief of police or his/her designee will conduct an annual review of the public safety camera system, its use, effectiveness and adherence to policy, including frequency and purpose for use of facial recognition or cognitive security software and frequency and purpose for retention of recordings beyond ninety (90) days, and will provide an annual information report to the city council regarding such review. ~~(Ord. 1007 § 2 (part), 2014).~~

2.56.090 Adoption of department policies.

The police department is directed to adopt policies to be included in its policy manual consistent with the provisions of this chapter, which policies may be more restrictive, but not less restrictive, than the policies set forth in this chapter. ~~(Ord. 1007 § 2 (part), 2014).~~

Policy
462

Menlo Park Police Department
Menlo Park PD Policy Manual

Automated License Plate Readers (ALPRs)

462.1 PURPOSE AND SCOPE

Best Practice

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. This policy is intended to assist the Menlo Park Police Department with:

- increasing public safety; minimizing the threat and risk of injury to individuals; promoting governmental legitimacy and accountability; minimizing the potential risks to individual privacy, civil rights, and civil liberties; protecting the integrity of the criminal investigatory, criminal intelligence and justice system processes and information; and increasing trust by maximizing transparency.

462.2 POLICY

Best Practice

The policy of the Menlo Park 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. The Menlo Park Police Department does not permit the sharing of ALPR data gathered by the City, vendors or subcontractors, as defined below, for:

(a) any purpose that violates this policy or any applicable laws and regulations;

(b) the purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code 7282.5: Government Code 7284.2 et seq) - these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP);

(c) any purpose that would assist another state to carry out enforcement actions that violate state or local laws.

For purposes of this policy, city contractors, vendors and subcontractors ("Contracted Entities") refers to any individual or entity that has a contract with the City related to ALPR technology. Prior to the Menlo Park Police Department sharing or giving access to ALPR data and technology to Contracted Entities, the City is required to enter into a written contract. Other law enforcement and governmental agencies are not considered Contracted Entities. The Menlo Park Police Department will only share and give access to ALPR data and technology to Contracted

Entities, law enforcement and governmental agencies, subject to the terms of this policy.

462.3 ADMINISTRATION

Best Practice MODIFIED

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates while recognizing the established privacy rights of the public. It is used by the Menlo Park 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. Such data is not open to public view, as it may contain confidential information.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Special Operations Commander. The Special Operations Commander 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

State MODIFIED

The Special Operations Commander shall be responsible for developing guidelines and procedures to comply with the requirements of Menlo Park's Municipal Code § 2.56 - Public Safety Information and Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.

(b) Training requirements for authorized users.

(c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws in compliance with Municipal Code § 2.56.

(d) Ensuring that accountability and transparency objectives are completed through the reporting of quarterly data to the public as assigned and maintaining the department's Transparency Portal to reflect ongoing ALPR system use.

(e) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52 and in compliance with Municipal Code § 2.56.

(f) The title and name of the current designee in overseeing the ALPR operation.

(g) Working with the Custodian of Records on the retention and destruction of ALPR data in compliance with Municipal Code § 2.56.030.

(h) Ensuring this policy and related procedures are conspicuously posted on the department's website.

462.4 OPERATIONS

State MODIFIED

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53; Municipal Code Chapter 2.56).

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

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass 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.

(d) No member of this department shall operate ALPR equipment or access ALPR data unless the purpose of such actions is allowed under this policy and only after completing department-approved training.

(e) Log in/ log out procedure. To ensure proper operation, facilitation, oversight and auditing of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data.

(f) Unless exigent circumstances exist, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator should confirm that the observed license plate from the ALPR system matches the license plate of the observed vehicle. Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated or unless exigent circumstances exist.

(g) Hot Lists- designation of hot lists, which are lists of vehicles determined to be criminally involved or associated with a missing person, to be utilized by the ALPR system shall be made by the ALPR Administrator or her/his designee. Occasionally, there may be errors in the LPR's system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Menlo Park Police Department members shall undertake the following steps:

1. Verification of status on a Hot List. An officer must receive confirmation from a communications dispatcher or other department computer device, that the license plate is still stolen, wanted or otherwise of interest before proceeding (absent exigent circumstances)

2. Visual verification of license plate number. Officers shall visually verify that the license plate of interest matches with the image of the license plate number captured (read) by the LPR, including both the alphanumeric characters of the license plate, state of issuance, and vehicle descriptors, before proceeding. Officers alerted to the fact that an observed motor vehicle's license plate is entered as a "Hot plate" or "hit" (a "hit" means the ALPR system has been alerted

to the involved license plate) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a reasonable basis exists before a Department member would have a lawful reason to stop the vehicle.

3. Department members will clear all stops from hot list alerts by indicating the positive ALPR hit, i.e. with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR hit and the arrest, then the Department member shall update the Communications Dispatcher.

4. General Hot Lists will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

5. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. Department issued Hot Lists shall be approved by the ALPR Administrator (or her/his designee) before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Department member's immediate supervisor. The hits from these data sources should be viewed as informational: created solely to bring the officers' attention to specific vehicles that have been associated with criminal activity or missing persons.

All Hot Plates and suspect information entered into the ALPR system will contain the following information at a minimum: Department member's name, related case number and a short synopsis describing the nature of the originating call for service. The member may add any additional information they deem to be relevant.

462.4.1 PERMITTED/ PROHIBITED USES

The ALPR system, and all data collected, is the property of the Menlo Park Police Department. Department personnel shall only access and use the ALPR system for official and legitimate law enforcement or public safety purposes consistent with this policy. Any official legitimate law enforcement or public safety purposes referenced in this policy shall be limited to purposes that comply with this policy and any applicable laws, including California Civil Code 1798.90.5 et seq (as amended). The following uses of the ALPR system are specifically prohibited:

(a) Invasion of Privacy: Except when done pursuant to a court order, such as a search warrant, it is prohibited to utilize the ALPR system 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 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 prohibited to use the ALPR system to harass and/or intimidate any individual or group.

(c) Use based on a protected characteristic: It is prohibited to use the ALPR system or associated files or Hot Lists solely based on a person's or group's race, gender, gender identity, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, age, or other classification protected by law.

(d) Personal Use: It is prohibited to use the ALPR system or associated files or Hot Lists for any

personal purpose.

(e) First Amendment Rights: It is prohibited to use the ALPR system or associated files or Hot Lists for the purpose or known effect of infringing upon First Amendment rights. Nothing in this policy is intended to create an independent right of action in any person.

Any member who engages in prohibited uses of the ALPR system, regarding the collection, receipt, access, use, dissemination, retention, or associated files or Hot Lists, may be subjected to: criminal prosecution; civil liability; and/or administrative sanctions and disciplinary action.

462.5 DATA COLLECTION AND RETENTION

Best Practice MODIFIED

The Special Operations Commander is 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 designated storage in accordance with department procedures. Data will be securely transmitted to the Flock Database, and/or to Northern California Regional Intelligence Center (NCRIC) as part of a multi-jurisdictional public safety program (Municipal Code § 2.56.030.)

Data transmitted from the police department shall be kept no more than thirty (30) days, and then destroyed (Municipal Code § 2.56.030.) 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.

Information gathered or collected and records retained by Contracted Entities, will not be sold, accessed or used for any reason other than legitimate law enforcement or public safety purposes. In accordance with this policy, data collected by ALPR cameras will not be accessed by Contracted Entities without prior authorization by the Chief of Police and/or her/his designee.

Any purging of data required under this policy must ensure that the data is completely purged and sanitized so that the data is not accessible or retrievable in any form including but not limited to being forensically recoverable.

462.6 ACCOUNTABILITY AND SAFEGUARDS

State MODIFIED

All data will be closely safeguarded and protected by both procedural and technological means. The Menlo Park 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; Municipal Code § 2.56.030):

(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-related civil or administrative

action.

(c) Every ALPR browsing inquiry must be documented by either the associated Menlo Park Police Department case number or incident number, and the reason for the inquiry.

(d) ALPR system audits should be conducted on a regular basis by the Special Operations Commander and violations of this policy shall be documented and steps should be taken to prevent such violations in the future.

(e) ALPR system audits shall be reflected in departmental quarterly reporting to the public.

(f) Annual ALPR audits will be conducted by an outside law enforcement agency as an added measure of transparency and to ensure policy compliance by members of the Menlo Park Police Department. If a violation of this policy is identified, it shall be documented and steps should be taken to prevent such violations in the future.

For security or data breaches, Menlo Park Police Department maintains a detailed policy for security and preservation of records. Please see the Records Maintenance and Release Policy.

462.7 RELEASING ALPR DATA

Best Practice MODIFIED

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, using the following procedures (Municipal Code § 2.56.030):

(a) The agency makes a written request for the ALPR data that includes:

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 Special Operations Commander or the authorized designee and approved before the request is fulfilled.

(c) The approved 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).

462.8 TRAINING

State

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

462.9 AUDITING AND REPORTING

Agency Content

The police department will provide an informational Quarterly Report to the City Council

summarizing ALPR activity by the department over the previous three months (Municipal Code § 2.56.050).

Menlo Park Police Department will establish and maintain a Transparency Portal for data collected through the Flock system, and provide access to the Transparency Portal through the department website.

ALPR system audits will be randomly conducted by the California Department of Justice and in conjunction with yearly CLETS audits.

462.10 CONTRACTED ENTITIES

All Contracted Entities are expected to comply with the relevant sections of this policy. Contracted Entities are also required to keep written documentation of who accesses the ALPR data and who the data is released to. Contracted Entities are prohibited from:

1. Sharing the ALPR data received from the City with any individual, entity or agency without express written permission from the Menlo Park Police Department.
2. Accessing, downloading, or decrypting the ALPR data received from the City without express written permission from the Menlo Park Police Department.
3. Storing the data in any form or length of time that violates this policy.
4. Allowing their employees, other than those with authorized authority, to access the ALPR data
5. Using the data in a manner that is not consistent with this policy or approved by the Menlo Park Police Department.

462.11 ALPR LOCATIONS

ALPR cameras approved by Council shall be located in areas of the City where there is a demonstrated need for the cameras to be placed. Placement of the cameras shall not be solely based on targeting any particular residential neighborhood or street, and it shall never be based on any protected characteristics or classifications.

Master Services Agreement

This Master Services Agreement (this "***Agreement***") is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Road NW Suite 210, Atlanta, GA 30318 ("***Flock***") and the entity identified in the signature block ("***Customer***") (each a "***Party***," and together, the "***Parties***") on this the ___ day of _____ 2024. This Agreement is effective on the date of mutual execution ("***Effective Date***"). Parties will sign an Order Form ("***Order Form***") which will describe the Flock Services to be performed and the period for performance, attached hereto as **Exhibit A**. The Parties agree as follows:

RECITALS

WHEREAS, Flock offers a software and hardware situational awareness solution through Flock's technology platform that upon detection is capable of capturing audio, video, image, and recording data and provide notifications to Customer ("***Notifications***");

WHEREAS, Customer desires access to the Flock Services (defined below) on existing devices, provided by Customer, or Flock provided Flock Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, via the Flock Services;

WHEREAS, Customer shall have access to the Footage in Flock Services. Pursuant to Flock's standard Retention Period (defined below) Flock deletes all Footage on a rolling thirty (30) day basis, except as otherwise stated on the ***Order Form***. Customer shall be responsible for extracting, downloading and archiving Footage from the Flock Services on its own storage devices; and

WHEREAS, Flock desires to provide Customer the Flock Services and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime; bona fide investigations; and evidence gathering for law enforcement purposes, ("***Permitted Purpose***").

AGREEMENT

NOW, THEREFORE, Flock and Customer agree that this Agreement, and any Order Form, purchase orders, statements of work, product addenda, or the like, attached hereto as exhibits and incorporated by reference, constitute the complete and exclusive statement of the Agreement of the Parties with respect to the subject matter of this Agreement, and replace and supersede all prior agreements, term sheets, purchase orders, correspondence, oral or written communications and negotiations by and between the Parties.

1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

1.1 "***Anonymized Data***" means Customer Data permanently stripped of identifying details and any potential personally identifiable information, by commercially available standards which irreversibly alters data in such a way that a data subject (i.e., individual person or entity) can no longer be identified directly or indirectly.

1.2 "***Authorized End User(s)***" means any individual employees, agents, or contractors of Customer accessing or using the Services, under the rights granted to Customer pursuant to this Agreement.

1.3 "***Customer Data***" means the data, media and content provided by Customer through the Services. For the avoidance of doubt, the Customer Data will include the Footage.

1.4. "***Customer Hardware***" means the third-party camera owned or provided by Customer and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Services.

1.5 "***Embedded Software***" means the Flock proprietary software and/or firmware integrated with or installed on the Flock Hardware or Customer Hardware.

1.6 "***Flock Hardware***" means the Flock device(s), which may include the pole, clamps, solar panel, installation components, and any other physical elements that interact with the Embedded Software and the Web Interface, to provide the Flock Services as specifically set forth in the applicable product addenda.

1.7 "***Flock IP***" means the Services, the Embedded Software, and any intellectual property or proprietary information therein or otherwise provided to Customer and/or its Authorized End Users. Flock IP does not include Footage (as defined below).

1.8 "***Flock Network End User(s)***" means any user of the Flock Services that Customer authorizes access to or receives data from, pursuant to the licenses granted herein.

1.9 "***Flock Services***" means the provision of Flock's software and hardware situational awareness solution, via the Web Interface, for automatic license plate detection, alerts, audio detection, searching image records, video and sharing Footage.

1.10 "***Footage***" means still images, video, audio and other data captured by the Flock Hardware or Customer Hardware in the course of and provided via the Flock Services.

1.11 *"**Hotlist(s)***" means a digital file containing alphanumeric license plate related information pertaining to vehicles of interest, which may include stolen vehicles, stolen vehicle license plates, vehicles owned or associated with wanted or missing person(s), vehicles suspected of being involved with criminal or terrorist activities, and other legitimate law enforcement purposes. Hotlist also includes, but is not limited to, national data (i.e., NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and includes manually entered license plate information associated with crimes that have occurred in any local jurisdiction.

1.12 "***Installation Services***" means the services provided by Flock for installation of Flock Services.

1.13 "***Retention Period***" means the time period that the Customer Data is stored within the cloud storage, as specified in the product addenda.

1.14 "***Vehicle Fingerprint*™**" means the unique vehicular attributes captured through Services such as: type, make, color, state registration, missing/covered plates, bumper stickers, decals, roof racks, and bike racks.

1.15 "***Web Interface***" means the website(s) or application(s) through which Customer and its Authorized End Users can access the Services.

2. SERVICES AND SUPPORT

2.1 **Provision of Access.** Flock hereby grants to Customer a non-exclusive, non-transferable right to access the features and functions of the Flock Services via the Web Interface during the Term, solely for the Authorized End Users. The Footage will be available for Authorized End Users to access and download via the Web Interface for the data retention time defined on the Order Form ("***Retention Period***"). Authorized End Users will be required to sign up for an account and select a password and username ("***User ID***"). Customer shall be responsible for all acts and omissions of Authorized End Users, and any act or omission by an Authorized End User which, including any acts or omissions of authorized End user which would constitute a breach of this agreement if undertaken by Customer. Customer shall undertake reasonable efforts to make all Authorized End Users aware of all applicable provisions of this Agreement and shall cause Authorized End Users to comply with such provisions. Flock may use the services of one or more third parties to deliver any part of the Flock Services, (such as using a third party to host the Web Interface for cloud storage or a cell phone provider for wireless cellular coverage). Flock will pass through any warranties that Flock receives from its third-party service providers to the extent that such warranties can be provided Customer.

2.2 **Embedded Software License.** Flock grants Customer a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Embedded Software as it pertains to Flock Services, solely as necessary for Customer to use the Flock Services.

2.3 **Support Services.** Flock shall monitor the Flock Services, and any applicable device health, in order to improve performance and functionality. Flock will use commercially reasonable efforts to respond to requests for support within seventy-two (72) hours. Flock will provide Customer with reasonable technical and on-site support and maintenance services in-person, via phone or by email at support@flocksafety.com (such services collectively referred to as ***"Support Services"***).

2.4 **Upgrades to Platform.** Flock may make any upgrades to system or platform that it deems necessary or useful to (i) maintain or enhance the quality or delivery of Flock's products or services to its agencies, the competitive strength of, or market for, Flock's products or services, such platform or system's cost efficiency or performance, or (ii) to comply with applicable law.

Parties understand that such upgrades are necessary from time to time and will not diminish the quality of the services or materially change any terms or conditions within this Agreement.

2.5 **Service Interruption.** Services may be interrupted in the event that: (a) Flock's provision of the Services to Customer or any Authorized End User is prohibited by applicable law; (b) any third-party services required for Services are interrupted; (c) if Flock reasonably believe Services are being used for malicious, unlawful, or otherwise unauthorized use; (d) there is a threat or attack on any of the Flock IP by a third party; or (e) scheduled or emergency maintenance ("***Service Interruption***"). Flock will make commercially reasonable efforts to provide written notice of any Service Interruption to Customer, to provide updates, and to resume providing access to Flock Services as soon as reasonably possible after the event giving rise to the Service Interruption is cured. Flock will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Customer or any Authorized End User may incur as a result of a Service Interruption. To the extent that the Service Interruption is not caused by Customer's direct actions or by the actions of parties associated with the Customer, the time will be tolled by the duration of the Service Interruption (for any continuous suspension lasting at least one full day). For example, in the event of a Service Interruption lasting five (5) continuous days, Customer will receive a credit for five (5) free days at the end of the Term.

2.6 **Service Suspension.** Flock may temporarily suspend Customer's and any Authorized End User's access to any portion or all of the Flock IP or Flock Service if (a) there is a threat or attack on any of the Flock IP by Customer; (b) Customer's or any Authorized End User's use of the Flock IP disrupts or poses a security risk to the Flock IP or any other customer or vendor of Flock; (c) Customer or any Authorized End User is/are using the Flock IP for fraudulent or illegal activities; (d) Customer has violated any term of this provision, including, but not limited to, utilizing Flock Services for anything other than the Permitted Purpose; or (e) any unauthorized access to Flock Services through Customer's account ("***Service Suspension***"). Customer shall not be entitled to any remedy for the Service Suspension period, including any reimbursement, tolling, or credit. If the Service Suspension was not caused by Customer, the Term will be tolled by the duration of the Service Suspension.

2.7 **Hazardous Conditions.** Flock Services do not contemplate hazardous materials, or other hazardous conditions, including, without limit, asbestos, lead, toxic or flammable substances. In

the event any such hazardous materials are discovered in the designated locations in which Flock is to perform services under this Agreement, Flock shall have the right to cease work immediately.

3. CUSTOMER OBLIGATIONS

3.1 **Customer Obligations.** Flock will assist Customer Authorized End Users in the creation of a User ID. Authorized End Users agree to provide Flock with accurate, complete, and updated registration information. Authorized End Users may not select as their User ID, a name that they do not have the right to use, or any other name with the intent of impersonation. Customer and Authorized End Users may not transfer their account to anyone else without prior written permission of Flock. Customer shall advise all Authorized End Users that they shall not share their account username or password information and must protect the security of the username and password. Unless otherwise stated and defined in this Agreement, Customer shall not designate Authorized End Users for persons who are not officers, employees, or agents of Customer. Customer shall require that Authorized End Users use Customer-issued email addresses for the creation of their User ID. Customer is responsible for any Authorized End User activity associated with its account. Customer shall ensure that Customer provides Flock with up to date contact information at all times during the Term of this Agreement. Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Flock Services. Customer shall (at its own expense) provide Flock with reasonable access and use of Customer facilities and Customer personnel in order to enable Flock to perform Services (such obligations of Customer are collectively defined as ***"Customer Obligations"***).

3.2 **Customer Representations.** Customer represents, that Customer shall use Flock Services only in compliance with this Agreement and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of data, video, photo, or audio content.

4. DATA USE AND LICENSING

4.1 **Customer Data.** As between Flock and Customer, all right, title and interest in the Customer Data, belong to and are retained solely by Customer. Customer hereby grants to Flock a limited, non-exclusive, royalty-free, irrevocable, worldwide license to use the Customer Data and

perform all acts as may be necessary for Flock to provide the Flock Services to Customer during the Term of this Agreement. Flock does not own and shall not sell Customer Data.

4.2 **Customer Generated Data.** Flock may provide Customer with the opportunity to post, upload, display, publish, distribute, transmit, broadcast, or otherwise make available, messages, text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, or other information or materials produced by Customer (**"*Customer Generated Data"***). Customer shall retain whatever legally cognizable right, title, and interest in Customer Generated Data. Customer understands and acknowledges that Flock has no obligation to monitor or enforce Customer's intellectual property rights of Customer Generated Data. Customer grants Flock a non-exclusive, irrevocable, worldwide, royalty-free, license to use the Customer Generated Data for the purpose of providing Flock Services. Flock does not own and shall not sell Customer Generated Data.

4.3 **Anonymized Data.** Subject to any City policy required pursuant to Civil Code section 1798.90.5 et seq., Flock shall have the right to collect, analyze, and anonymize Customer Data and Customer Generated Data to the extent such anonymization renders the data non-identifiable to create Anonymized Data to use and perform the Services and related systems and technologies, including the training of machine learning algorithms. Customer hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right to use and distribute such Anonymized Data to improve and enhance the Services and for other development, diagnostic and corrective purposes, and other Flock offerings. Parties understand that the aforementioned license is required for continuity of Services. Flock does not own and shall not sell Anonymized Data.

5. CONFIDENTIALITY; DISCLOSURES

5.1 **Confidentiality.** To the extent required by any applicable public records requests, each Party (the "***Receiving Party***") understands that the other Party (the "***Disclosing Party***") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "***Proprietary Information***" of the Disclosing Party). Proprietary Information of Flock includes non-public information regarding features, functionality and performance of the Services. Proprietary Information of Customer includes non-public data provided by Customer to Flock or collected by Flock via Flock Services, which

includes but is not limited to geolocation information and environmental data collected by sensors. The Receiving Party agrees: (i) to take the same security precautions to protect against disclosure or unauthorized use of such Proprietary Information that the Party takes with its own proprietary information, but in no event less than commercially reasonable precautions, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public; or (b) was in its possession or known by it prior to receipt from the Disclosing Party; or (c) was rightfully disclosed to it without restriction by a third party; or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. At the termination of this Agreement, all Proprietary Information will be returned to the Disclosing Party, destroyed or erased (if recorded on an erasable storage medium), together with any copies thereof, when no longer needed for the purposes above, or upon request from the Disclosing Party, and in any case upon termination of the Agreement. Notwithstanding any termination, all confidentiality obligations of Proprietary Information that is trade secret shall continue in perpetuity or until such information is no longer trade secret.

5.2 **Usage Restrictions on Flock IP.** Flock and its licensors retain all right, title and interest in and to the Flock IP and its components, and Customer acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement. Customer further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion. Customer and Authorized End Users shall not: (i) copy or duplicate any of the Flock IP; (ii) decompile, disassemble, reverse engineer, or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock IP is compiled or interpreted, or apply any other process or procedure to derive the source code of any software included in the Flock IP; (iii) attempt to modify, alter, tamper with or repair any of the Flock IP, or attempt to create any derivative product from any of the foregoing; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock IP; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right

appearing on or contained within the Flock Services or Flock IP; (vi) use the Flock Services for anything other than the Permitted Purpose; or (vii) assign, sublicense, sell, resell, lease, rent, or otherwise transfer, convey, pledge as security, or otherwise encumber, Customer's rights. There are no implied rights.

5.3 **Disclosure of Footage.** Subject to and during the Retention Period, Flock may access, use, preserve and/or disclose the Footage if Flock is compelled by law to do so.

6. PAYMENT OF FEES

6.1 **Billing and Payment of Fees**. Customer shall pay the fees set forth in the applicable Order Form based on the billing structure and payment terms as indicated in the Order Form. If Customer believes that Flock has billed Customer incorrectly, Customer must contact Flock no later than thirty (30) days after the closing date on the first invoice in which the error or problem appeared to receive an adjustment or credit. Customer acknowledges and agrees that a failure to contact Flock within this period will serve as a waiver of any claim. If any undisputed fee is more than thirty (30) days overdue, Flock may, without limiting its other rights and remedies, suspend delivery of its service until such undisputed invoice is paid in full. Flock shall provide at least thirty (30) days' prior written notice to Customer of the payment delinquency before exercising any suspension right.

6.2 **Notice of Changes to Fees.** Flock reserves the right to change the fees for subsequent Renewal Terms by providing sixty (60) days' notice (which may be sent by email) prior to the end of the Initial Term or Renewal Term (as applicable).

6.3 **Late Fees.** If payment is not issued to Flock by the due date of the invoice, an interest penalty of 1.0% of any unpaid amount may be added for each month or fraction thereafter, until final payment is made.

6.4 **Taxes.** Customer is responsible for all taxes, levies, or duties, excluding only taxes based on Flock's net income, imposed by taxing authorities associated with the order. If Flock has the legal obligation to pay or collect taxes, including amount subsequently assessed by a taxing authority, for which Customer is responsible, the appropriate amount shall be invoice to and paid by Customer unless Customer provides Flock a legally sufficient tax exemption certificate and Flock shall not charge customer any taxes from which it is exempt. If any deduction or withholding is required by law, Customer shall notify Flock and shall pay Flock any additional

amounts necessary to ensure that the net amount that Flock receives, after any deduction and withholding, equals the amount Flock would have received if no deduction or withholding had been required.

7. TERM AND TERMINATION

7.1 **Term.** The initial term of this Agreement shall be for the period of time set forth on the Order Form (the "***Term***"). Following the Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms of one (1) year ("***Renewal Term***") unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.

7.2 **Termination.** Upon termination or expiration of this Agreement, Flock will remove any applicable Flock Hardware at a commercially reasonable time period. In the event of any material breach of this Agreement, the non-breaching Party may terminate this Agreement prior to the end of the Term by giving thirty (30) days prior written notice to the breaching Party; provided, however, that this Agreement will not terminate if the breaching Party has cured the breach prior to the expiration of such thirty (30) day period ("***Cure Period***"). Either Party may terminate this Agreement (i) upon the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other Party's making an assignment for the benefit of creditors, or (iii) upon the other Party's dissolution or ceasing to do business. In the event of a material breach by Flock, and Flock is unable to cure within the ***Cure Period***, Flock will refund Customer a pro-rata portion of the pre-paid fees for Services not received due to such termination.

7.3 **Survival**. The following Sections will survive termination: 1, 3, 5, 6, 7, 8.3, 8.4, 9, 11.1 and 11.6.

8. REMEDY FOR DEFECT; WARRANTY AND DISCLAIMER

8.1 **Manufacturer Defect.** Upon a malfunction or failure of Flock Hardware or Embedded Software (a **"*Defect*"**), Customer must notify Flock's technical support team. In the event of a Defect, Flock shall make a commercially reasonable attempt to repair or replace the defective Flock Hardware at no additional cost to the Customer. Flock reserves the right, in its sole discretion, to repair or replace such Defect, provided that Flock shall conduct inspection or testing within a commercially reasonable time, but no longer than seven (7) business days after Customer gives notice to Flock.

8.2 **Replacements.** In the event that Flock Hardware is lost, stolen, or damaged, Customer may request a replacement of Flock Hardware at a fee according to the reinstall fee schedule (https://www.flocksafety.com/reinstall-fee-schedule). In the event that Customer chooses not to replace lost, damaged, or stolen Flock Hardware, Customer understands and agrees that (1) Flock Services will be materially affected, and (2) that Flock shall have no liability to Customer regarding such affected Flock Services, nor shall Customer receive a refund for the lost, damaged, or stolen Flock Hardware.

8.3 **Warranty.** Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of other causes beyond Flock's reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

8.4 **Disclaimer.** THE REMEDY DESCRIBED IN SECTION 8.1 ABOVE IS CUSTOMER'S SOLE REMEDY, AND FLOCK'S SOLE LIABILITY, WITH RESPECT TO DEFECTS. FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED "AS IS" AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 11.6.

8.5 **Insurance.** Flock will maintain commercial general liability policies as stated in Exhibit B.

8.6 **Force Majeure.** Parties are not responsible or liable for any delays or failures in performance from any cause beyond their control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, pandemics (including the spread of variants), issues of national security, acts or omissions of third-party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, supply chain shortages of equipment or supplies, financial institution crisis, weather conditions or acts of hackers, internet service providers or any other third party acts or omissions.

9. LIMITATION OF LIABILITY; INDEMNITY

9.1 **Limitation of Liability.** NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK, ITS OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR LOSS OF REVENUE, BUSINESS OR BUSINESS INTERRUPTION OF CUSTOMER; (B) INCOMPLETE, CORRUPT, OR INACCURATE DATA; (C) COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY; (D) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (E) FOR ANY MATTER BEYOND FLOCK'S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY CUSTOMER TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWENTY-FOUR (24) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SECTION ONLY

APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE REFERENCED IN SECTION 10.6. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE FOREGOING LIMITATIONS OF LIABILITY SHALL NOT APPLY (I) IN THE EVENT OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (II) INDEMNIFICATION OBLIGATIONS IN SECTION 9.3.

9.2 **Responsibility.** Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable for the torts of its own officers, agents, or employees.

9.3 **Flock Indemnity.** To the fullest extent permitted by law, Flock shall defend (with legal counsel reasonably acceptable to Customer), indemnify and hold harmless Customer and its officers, elected officials, employees, agents, and volunteers (collectively "Indemnitees") from and against any and all claims, loss, cost, damage, injury (including, without limitation, injury to or death of an employee of Flock or its subconsultants), expense and liability of every kind, nature and description (including, without limitation, fines, penalties, incidental and consequential damages, reasonable court costs and attorneys' fees, litigation expenses and fees of expert consultants or expert witnesses incurred in connection therewith, and costs of investigation, costs incurred related to breach of information security for which notice must be given pursuant to Civil Code section 1798.82 or 1798.29), where the same arise out of, are a consequence of or are in any way attributable to, in whole or in part, the performance of this Agreement by Flock or by any individual or entity for whom Flock is legally liable, including but not limited to, Flock's officers, agents, employees, subcontractors or consultants of Flock. The termination of this Agreement or the completion of Services or the Installation Services contemplated herein shall not release Flock from its obligations under this section, as long as the event giving rise to the claim, damage, injury, expense or liability occurred prior to the effective date of any such termination or completion, and this section shall survive the termination of the Agreement.

10. INSTALLATION SERVICES AND OBLIGATIONS

10.1 **Ownership of Hardware**. Flock Hardware is owned and shall remain the exclusive property of Flock. Title to any Flock Hardware shall not pass to Customer upon execution of this

Agreement, except as otherwise specifically set forth in this Agreement. Except as otherwise expressly stated in this Agreement, Customer is not permitted to remove, reposition, re-install, tamper with, alter, adjust or otherwise take possession or control of Flock Hardware. Customer agrees and understands that in the event Customer is found to engage in any of the foregoing restricted actions, all warranties herein shall be null and void, and this Agreement shall be subject to immediate termination for material breach by Customer. Customer shall not perform any acts which would interfere with the retention of title of the Flock Hardware by Flock. Should Customer default on any payment of the Flock Services, Flock may remove Flock Hardware at Flock's discretion. Such removal, if made by Flock, shall not be deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Customer's default and Flock shall have the right to enforce any other legal remedy or right.

10.2 **Deployment Plan**. Flock shall advise Customer on the location and positioning of the Flock Hardware for optimal product functionality, as conditions and locations allow. Flock will collaborate with Customer to design the strategic geographic mapping of the location(s) and implementation of Flock Hardware to create a deployment plan ("***Deployment Plan***"). In the event that Flock determines that Flock Hardware will not achieve optimal functionality at a designated location, Flock shall have final discretion to veto a specific location, and will provide alternative options to Customer.

10.3 **Changes to Deployment Plan.** After installation of Flock Hardware, any subsequent requested changes to the Deployment Plan, including, but not limited to, relocating, re-positioning, adjusting of the mounting, removing foliage, replacement, changes to heights of poles will incur a fee according to the reinstall fee schedule located at (https://www.flocksafety.com/reinstall-fee-schedule). Customer will receive prior notice and confirm approval of any such fees.

10.4 **Customer Installation Obligations**. Customer is responsible for any applicable supplementary cost as described in the Customer Implementation Guide, attached hereto as Exhibit C ("***Customer Obligations***"). Customer represents and warrants that it has, or shall lawfully obtain, all necessary right title and authority and hereby authorizes Flock to install the Flock Hardware at the designated locations and to make any necessary inspections or maintenance in connection with such installation.

10.5 **Flock's Obligations**. Installation of any Flock Hardware shall be installed in a professional manner within a commercially reasonable time from the Effective Date of this Agreement. Upon removal of Flock Hardware, Flock shall restore the location to its original condition, ordinary wear and tear excepted. Flock will continue to monitor the performance of Flock Hardware for the length of the Term. Flock may use a subcontractor or third party to perform certain obligations under this agreement, provided that Flock's use of such subcontractor or third party shall not release Flock from any duty or liability to fulfill Flock's obligations under this Agreement.

11. MISCELLANEOUS

11.1 **Compliance With Laws.** Parties shall comply with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules, including responding to any subpoena request(s).

11.2 **Severability.** If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect.

11.3 **Assignment.** This Agreement is not assignable, transferable or sublicensable by either Party, without prior consent. Notwithstanding the foregoing, either Party may assign this Agreement, without the other Party's consent, (i) to any parent, subsidiary, or affiliate entity, or (ii) to any purchaser of all or substantially all of such Party's assets or to any successor by way of merger, consolidation or similar transaction.

11.4 **Entire Agreement.** This Agreement, together with the Order Form(s), the reinstall fee schedule (https://www.flocksafety.com/reinstall-fee-schedule), and any attached exhibits are the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous or contemporaneous negotiations, discussions or agreements, whether written or oral, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both Parties, except as otherwise provided herein. None of Customer's purchase orders, authorizations or similar documents will alter the terms of this Agreement, and any such conflicting terms are expressly rejected. Any mutually agreed upon purchase order is subject to these terms. In the event of any conflict of terms found in this Agreement or any other terms and conditions, the

terms of this Agreement shall prevail. Customer agrees that Customer's purchase is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written comments made by Flock with respect to future functionality or feature.

11.5 **Relationship.** No agency, partnership, joint venture, or employment is created as a result of this Agreement and Parties do not have any authority of any kind to bind each other in any respect whatsoever. Flock shall at all times be and act as an independent contractor to Customer.

11.6 **Governing Law; Venue.** This Agreement shall be governed by the laws of the state in which the Customer is located. The Parties hereto agree that venue would be proper in the chosen courts of the State of which the Customer is located. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.

11.7 **Special Terms.** Flock may offer certain special terms which are indicated in the proposal and will become part of this Agreement, upon Customer's prior written consent and the mutual execution by authorized representatives ("***Special Terms***"). To the extent that any terms of this Agreement are inconsistent or conflict with the Special Terms, the Special Terms shall control.

11.8 **Publicity.** Flock has the right to reference and use Customer's name and trademarks and disclose the nature of the Services in business and development and marketing efforts.

11.9 **Feedback.** If Customer or Authorized End User provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency or Authorized End User hereby assigns to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

11.10 **Export.** Customer may not remove or export from the United States or allow the export or re-export of the Flock IP or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign Customer or authority. As defined in Federal Acquisition Regulation ("FAR"), section 2.101, the Services, the Flock Hardware and Documentation are "commercial items" and according to the Department of Defense Federal Acquisition Regulation ("DFAR") section 252.2277014(a)(1) and are deemed to be "commercial computer software" and "commercial computer software documentation." Flock is compliant with FAR Section 889 and does not

contract or do business with, use any equipment, system, or service that uses the enumerated banned Chinese telecommunication companies, equipment or services as a substantial or essential component of any system, or as critical technology as part of any Flock system. Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

11.11 **Headings.** The headings are merely for organization and should not be construed as adding meaning to the Agreement or interpreting the associated sections.

11.12 **Authority.** Each of the below signers of this Agreement represent that they understand this Agreement and have the authority to sign on behalf of and bind the Parties they are representing.

11.13 **Conflict.** In the event there is a conflict between this Agreement and any applicable statement of work, or Customer purchase order, this Agreement controls.

11.14 **Public Disrepute.** In the event Customer or its employees become the subject of an indictment, arrest, public disrepute, contempt, scandal, or behaves in a manner that, in the reasonable judgment of Flock, reflects unfavorably upon Flock, and/or their officers or principals, licensees, such act(s) or omission(s) shall constitute a material breach of this Agreement and Flock shall, in addition to any other rights and remedies available to it hereunder, whether at law or in equity, have the right to elect to terminate this Agreement.

11.15 **Notices.** All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

FLOCK NOTICES ADDRESS:

1170 HOWELL MILL ROAD, NW SUITE 210

ATLANTA, GA 30318

ATTN: LEGAL DEPARTMENT

EMAIL: legal@flocksafety.com

Customer NOTICES ADDRESS:

ADDRESS: _____

ATTN: _____

EMAIL: _____

EXHIBIT A

ORDER FORM

EXHIBIT B

INSURANCE

Required Coverage. Flock shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property that may arise from or in connection with the performance of the services under this Agreement and the results of that work by Flock or its agents, representatives, employees or subcontractors. Insurance shall be placed with insurers with a current A. M. Best rating of no less than "A" and "VII". Flock shall obtain and, during the term of this Agreement, shall maintain policies of professional liability (errors and omissions), automobile liability, and general liability insurance for insurable amounts of not less than the limits listed herein. The insurance policies shall provide that the policies shall remain in full force during the life of the Agreement.

Types and Amounts Required. Flock shall maintain, at minimum, the following insurance coverage for the duration of this Agreement:

(i) **Commercial General Liability** insurance written on an occurrence basis with minimum limits of One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) in the aggregate for bodily injury, death, and property damage, including personal injury, contractual liability, independent contractors, broad-form property damage, and product and completed operations coverage, at least as broad as Insurance Service Office Form CG 00 01;

(ii) **Umbrella or Excess Liability** insurance written on an occurrence basis with minimum limits of Ten Million Dollars ($10,000,000) per occurrence and Ten Million Dollars ($10,000,000) in the aggregate;

(iii) **Professional Liability/Errors and Omissions** insurance with minimum limits of Five Million Dollars ($5,000,000) per occurrence and Five Million Dollars ($5,000,000) in the aggregate;

(iv) **Commercial Automobile Liability** insurance with a minimum combined single limit of One Million Dollars ($1,000,000) per occurrence for bodily injury, death, and property coverage, including owned and non-owned and hired automobile coverage; and

(v) **Cyber Liability** insurance written on an occurrence basis with minimum limits of Five Million Dollars ($5,000,000). Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Vendor in this agreement and shall include, but not be limited

to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

(vi) Workers' Compensation: as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than One Million Dollars ($1,000,000) per accident for bodily injury or disease.

Flock shall furnish the Customer with original certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this Exhibit. All certificates and endorsements are to be received and approved by the Customer before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive Flock's obligation to provide them. The Customer reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.

The insurance policies are to contain, or be endorsed to contain, the following provisions:

The City of Menlo Park, its Council Members, directors, officers, agents and employees shall be named as additional insureds on the CGL and Workers' Compensation policies with respect to liability arising out of work or operations performed by or on behalf of Flock including materials, parts or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to Flock's insurance (at least as broad as ISO Form CG 20 10 11 85 or both CG 20 10, CG 20 26, CG 20 33, or CG 20 38; and CG 20 37 forms if later revisions used).
For any claims related to this contract, Flock's insurance coverage shall be primary insurance coverage (at least as broad as ISO CG 20 01 04 13) with respect to the Customer, its officers, officials, employees, and volunteers. Any insurance or self-insurance maintained by the

Customer, its officers, officials, employees, or volunteers shall be excess of the Flock's insurance and shall not contribute with it.

Flock hereby grants to Customer a waiver of any right to subrogation which any insurer of Flock may acquire against the City by virtue of the payment of any loss under such insurance. Flock agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the Customer has received a waiver of subrogation endorsement from the insurer.

Flock shall require the insurer to provide Customer with thirty (30) days' prior notice of termination or material change in coverage and ten (10) days prior notice of cancellation for non-payment.

EXHIBIT C

CUSTOMER OBLIGATIONS

Flock Safety + CA - Menlo Park PD

Flock Group Inc.
1170 Howell Mill Rd, Suite 210
Atlanta, GA 30318

MAIN CONTACT:
Tariq Bright
tariq.bright@flocksafety.com
4088968551

Created Date: 09/25/2024
Expiration Date: 10/24/2024
Quote Number: Q-79344
PO Number:

flock safety

flock safety

Budgetary Quote

This document is for informational purposes only. Pricing is subject to change.

Bill To: 701 Laurel St Menlo Park, California 94025

Ship To: 701 Laurel St Menlo Park, California 94025

Billing Company Name: CA - Menlo Park PD
Billing Contact Name:
Billing Email Address:
Billing Phone:

Subscription Term: 24 Months
Payment Terms: Net 30
Retention Period: 30 Days
Billing Frequency: Annual Plan - First Year Invoiced at Signing.

Hardware and Software Products

Annual recurring amounts over subscription term

Item	Cost	Quantity	Total
Flock Safety Platform			**$112,500.00**
Flock Safety Flock OS			
FlockOS ™ - Essentials	Included	1	Included
Enhanced LPR Upgrade	Included	1	Included
Flock Safety LPR Products			
Flock Safety Falcon ®	Included	35	Included

Professional Services and One Time Purchases

Item	Cost	Quantity	Total
One Time Fees			
Flock Safety Professional Services			
Professional Services - Standard Implementation Fee	$650.00	13	$8,450.00
Professional Services - Existing Infrastructure Implementation Fee	$150.00	17	$2,550.00
Professional Services - Advanced Implementation Fee	$1,900.00	5	$9,500.00

Subtotal Year 1:	$133,000.00
Annual Recurring Subtotal:	$112,500.00
Estimated Tax:	$0.00
Contract Total:	$245,500.00

Taxes shown above are provided as an estimate. Actual taxes are the responsibility of the Customer. This is not an invoice – this document is a non-binding proposal for informational purposes only. Pricing is subject to change.

Billing Schedule	Amount (USD)
Year 1	
At Contract Signing	$133,000.00
Annual Recurring after Year 1	$112,500.00
Contract Total	$245,500.00

*Tax not included

Product and Services Description

FlockOS Features	Description
FlockOS ™ - Essentials	An integrated public safety platform that detects, centralizes and decodes actionable evidence to increase safety, improve efficiency, and connect the community.
Enhanced LPR Upgrade	The Enhanced LPR Package is a software add-on for any of the FlockOS® tiers designed to help detectives and patrol officers conduct more efficient, informed, and collaborative investigations. Its advanced License Plate Recognition (LPR) features streamline investigations, providing officers with immediate access to essential information and improving communication within and across departments.
Flock Safety Falcon ®	Law enforcement grade infrastructure-free (solar power + LTE) license plate recognition camera with Vehicle Fingerprint ™ technology (proprietary machine learning software) and real-time alerts for unlimited users.
Professional Services - Standard Implementation Fee	One-time Professional Services engagement. Includes site and safety assessment, camera setup and testing, and shipping and handling in accordance with the Flock Safety Standard Implementation Service Brief.
Professional Services - Existing Infrastructure Implementation Fee	One-time Professional Services engagement. Includes site and safety assessment of existing vertical infrastructure location, camera setup and testing, and shipping and handling in accordance with the Flock Safety Standard Implementation Service Brief.
Professional Services - Advanced Implementation Fee	One-time Professional Services engagement. Includes site & safety assessment, camera setup & testing, and shipping & handling in accordance with the Flock Safety Advanced Implementation Service Brief.

FlockOS Features & Description

FlockOS Features	Description
Community Network Access	The ability to request direct access to feeds from privately owned Flock Safety Falcon® LPR cameras located in neighborhoods, schools, and businesses in your community, significantly increasing actionable evidence that clears cases.
Unlimited Users	Unlimited users for FlockOS
State Network (License Plate Lookup Only)	Allows agencies to look up license plates on all cameras opted into the Flock Safety network within your state.
Nationwide Network (License Plate Lookup Only)	With the vast Flock Safety sharing network, law enforcement agencies no longer have to rely on just their devices alone. Agencies can leverage a nationwide system boasting 10 billion additional plate reads per month to amplify the potential to collect vital evidence in otherwise dead-end investigations.
Law Enforcement Network Access	The ability to request direct access to evidence detection devices from Law Enforcement agencies outside of your jurisdiction.
Time & Location Based Search	Search full, partial, and temporary plates by time at particular device locations
License Plate Lookup	Look up specific license plate location history captured on Flock devices
Vehicle Fingerprint Search	Search footage using Vehicle Fingerprint™ technology. Access vehicle type, make, color, license plate state, missing / covered plates, and other unique features like bumper stickers, decals, and roof racks.
Insights & Analytics	Reporting tool to help administrators manage their LPR program with device performance data, user and network audits, plate read reports, hot list alert reports, event logs, and outcome reports.
ESRI Based Map Interface	Map-based interface that consolidates all data streams and the locations of each connected asset, enabling greater situational awareness and a common operating picture.
Real-Time NCIC Alerts on Flock ALPR Cameras	Receive automated alerts when vehicles entered into established databases for missing and wanted persons are detected, including the FBI's National Crime Information Center (NCIC) and National Center for Missing & Exploited Children (NCMEC) databases.
Unlimited Custom Hot Lists	Ability to add a suspect's license plate to a custom list and get alerted when it passes by a Flock camera
Convoy Search	Unearth hidden connections by detecting suspect vehicles that frequently travel together. This tool

	is invaluable for investigating organized or serial crimes and identifying accomplices.
Visual Search	Transforms any digital photo into a potent investigative lead, enhancing evidence collection. Upload the image of a vehicle into FlockOS® to initiate a reverse image search that will help you identify crucial suspect vehicle information and unlock dead-end investigations.
Multi Geo Search	Connects the dots between multiple crimes and crime scenes. Link a suspect vehicle to multiple incidents based on location, without needing a vehicle description or plate number.
Custom Hot List Attachments	The ability to add case notes, photos, reports, and other relevant case information to Custom Hot List Alerts
Custom Hot List Deconfliction	Allows Flock Safety users to identify overlapping investigations within their agency and within other law enforcement agencies and provide the contact information of opted-in parties to facilitate collaboration.
Unlimited Vehicle Description Alerts	Users can set up and receive notifications for suspect vehicles based on body type, make, color, location and timeframe. Notifications are sent via app, SMS or email when a vehicle matching the predetermined criteria passes a camera in your organization's network.