Surveillance Technology Policy

Automated License Plate Readers (ALPR)
Airport

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Automated License Plate Readers (ALPR) itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Department's mission is to: SFO's mission is to provide an exceptional airport in service to our communities.

The Surveillance Technology Policy ("Policy") defines the manner in which the Automated License Plate Readers (ALPR) will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Automated License Plate Readers (ALPR), including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of Automated License Plate Readers (ALPR) technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

Locate stolen, wanted, and or other vehicles that are the subject of investigation
To support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including the San Mateo County District Attorney's Office.
To locate victims, witnesses, suspects, and others associated with a law enforcement investigation.

- On an annual basis, the Department will evaluate the impact of the technology on the following measures:

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

BUSINESS JUSTIFICATION

Automated License Plate Readers (ALPR) supports the Department's mission and provides important operational value in the following ways:

Primary ALPR provides for a secondary capture of permitted operator activity at the airport, if the primary AVI malfunctions and fails to read the airport affixed transponder. Additional uses include tracking illegal operators who solicit for rides; assisting SFPD in an investigation.

In addition, Automated License Plate Readers (ALPR) promises to benefit residents in the following ways:

- ☐ Education
- ☐ Community Development
- ☐ Health
- ☐ Environment
- ☐ Criminal Justice
- ☐ Jobs
- ☐ Housing
- ☑ Other — Trip fees by permitted operators; Traffic congestion studies

Automated License Plate Readers (ALPR) will benefit the department in the following ways:

Benefit		Description	Quantity
☑	Financial Savings		
☑	Time Savings	Without the ALPR technology, the Airport would need to deploy a manually staffed ground transportation operations. This alternative has not been thoroughly explored for feasibility. At minimum however, team members would be required assignment at all entry lanes, exit lanes, curbside zones, and staging lots during a 24/7 operations. Team members would conduct manual verification of registration through visual observance of permits and decals, and conduct traffic counts. The Electronic Toll Readers removes the necessity of staffing for this purpose.	
☐	Staff Safety		
☐	Data Quality		
☑	Other		

Other benefits include

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy;

must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.	
Specifications:	The software and/or firmware used to operate the surveillance technology must be kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc. The surveillance technology collects the following data types and formats: • Video in MOV format • Still images from cameras in PDF format The surveillance technology collects the following data types: *Data Type(s)* *Format(s)* *Classification* Select...
Notification:	Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection. Department includes the following items in its public notice: ☐ Information on the surveillance technology ☐ Description of the authorized use ☐ Type of data collected ☐ Will persons be individually identified

	☐ Data retention ☐ Department identification ☐ Contact information
Access:	All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): *A. Department employees* Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology. • The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional: • *B. Members of the public* Airport will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules. Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants. Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.
Data Security:	Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

	To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:
Data Sharing:	Airport will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules. Airport will endeavor to ensure that other agencies or departments that may receive data collected by ALPR will act in conformity with this Surveillance Technology Policy. For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy. Airport shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security) Airport shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: ☐ Confirm the purpose of the data sharing aligns with the department's mission. ☐ Consider alternative methods other than sharing data that can accomplish the same purpose. ☐ Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. ☐ Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents. ☐ Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance. ☐ Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format. The Department currently participates in the following sharing practices:

	A. Internal Data Sharing Department shares the following data with the recipients:The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco. Data sharing occurs at the following frequency: B. External Data Sharing Department shares the following data with the recipients: The department does not share surveillance technology data externally with entities outside the City and County of San Francisco. Data sharing occurs at the following frequency: To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:
Data Retention:	Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories: • Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely • Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years • Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years The Department's data retention period and justification are as follows: PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s): Departments must establish appropriate safeguards for PII data stored for longer periods. Data will be stored in the following location: ☐ Local storage ☐ Department of Technology Data Center ☐ Software as a Service Product ☐ Could Storage Provider

Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Practices: Processes and Applications:
Training:	To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures. At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

Sanctions for violations of this Policy include the following:

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

Personally Identifiable Information:	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Raw Data:	Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Public:

Complaints or concerns can be submitted to the Department by

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

Automated License Plate Recognition (ALPR) technology shall be used to automate the processing of vehicle license plate information by transforming images into alphanumeric characters with optical recognition software and storing those images, plate information and related metadata, including time and geo-location information.
Automated License Plate Recognition (ALPR) technology automates the processing of vehicle license plates. Specifically, ALPR:

- uses specially designed cameras mounted on gantries at the airport's entry points to capture digital images of approaching vehicles as they drive into the airport. The database records images and compares them with known operators;
- transforms the images into alphanumeric characters with optical character recognition (OCR) software;
- stores the images, plate information, and related metadata in a restricted-access database;
- compares the transformed license plate characters to databases of AVI reads for billing purposes;
- archives photo evidence and metadata in support of citations issued ("hits") according to evidence retention standards consistent with City and State law;

The Landside division currently has one (1) P357, side-fire camera and (20) 3M PIPS P392+ Spikelet cameras.

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Technology Use:

Primary ALPR provides for a secondary capture of permitted operator activity at the airport, if the primary AVI malfunctions and fails to read the airport affixed transponder. Additional uses include tracking illegal operators who solicit for rides; assisting SFPD in an investigation.

PII:

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Locate stolen, wanted, and or other vehicles that are the subject of investigation

To support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including the San Mateo County District Attorney's Office.

To locate victims, witnesses, suspects, and others associated with a law enforcement investigation.

Rules:

Prohibited Uses:

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type	Formats STP

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.
Employee Job Classification & Title: Department: If applicable, contractor or vendor name: Rules and processes required prior to data access or use:
6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.
7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period
Retention: Reason for retention: Deletion process: Retention exemption conditions:
8. How collected information can be accessed or used by members of the public, including criminal defendants
Will the data be accessible to the public: How it can be accessed:
9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.
Name of agency: Justification:
10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology
Training required:

Description of training:
11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy
Training required: Process for responding to complaints: Oversight process: Compliance personnel titles: , Restrictions:
12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.
Complaint procedures: Departmental follow-up process: *Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org.*