Surveillance Technology Policy

San Francisco International Airport
Automated License Plate Readers (ALPR) – Ground Transportation Management System (GTMS)

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") – Ground Transportation Management System ("GTMS") 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 ("SFO" or "Airport") mission is to provide an exceptional airport in service to our communities.

The Surveillance Technology Policy ("Policy") defines the manner in which the ALPR – GTMS 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 ALPR – GTMS, 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 ALPR – GTMS technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. To track the activity of permitted commercial ground transportation at the Airport. Also used as a secondary method for collecting trip fees in the event an operator's transponder fails to read.
2. To support the Airport and local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of investigations, including locating stolen, wanted, and or other vehicles that are the subject of investigation; and/or locating victims, witnesses, suspects, and others associated with a law enforcement investigation.

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

Departments may use information collected only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally,

departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

ALPR – GTMS supports the Department's mission and provides important operational value in the following ways:

The Airport has historically used electronic toll readers and other technologies to monitor commercial ground transportation activity at the Airport. The PIPS Technology™ ("PIPS") ALPR – GTMS solution serves as a secondary source of ensuring commercial ground transportation database information is correct. This is an essential component of a comprehensive and efficient transportation system. Ground transportation activity at the Airport continues to grow in line with air passenger activity. In FY2019, there were over 6,500 (non TNC) vehicles permitted to operate at the Airport, with almost 3,000,000 pickups and drop-offs completed.

The primary use for Landside ALPR – GTMS is to capture the activity of permitted commercial ground transportation at the Airport. The ALPR – GTMS acts as a failsafe if the Automated Vehicle Identification (AVI) readers malfunctions and fails to read the transponder the Airport affixes to certain types of permitted vehicles. It assists in dispute resolution in the event that the operator challenges the transponder data (i.e., number of trips the operator has made to the Airport) collected from the AVI.

Additional uses include tracking permitted operators that are not issued transponders, such as TNC vehicles and long distance bus carriers; tracking unpermitted operators who solicit passengers for rides; and assisting public safety agencies in investigations.

In addition, ALPR – GTMS promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
X	Environment	Traffic congestion studies: ALPR – GTMS can be used to conduct studies on traffic volumes and patterns, with the potential to mitigate environmental impacts of traffic congestion on residents.
X	Criminal Justice	ALPR – GTMS can be used to support identification of vehicles as a part of law enforcement investigations.
☐	Jobs	
☐	Housing	
X	Other	Public Safety: ALPR – GTMS can be used to locate stolen, wanted, and or other vehicles that are the subject of investigation, and can improve overall roadway safety for residents using Airport roadways.

	Trip fees by permitted operators: ALPR – GTMS can be used to track vehicles and collect trip fees to offset impacts of commercial vehicles on Airport roadways and to improve roadway conditions for residents accessing the Airport.

In addition, the following benefits are obtained:

Benefit		Description
☐	Financial Savings	
X	Time Savings	Without the ALPR – GTMS technology, the Airport would need to deploy a manually staffed ground transportation operation. This alternative has not been thoroughly explored for feasibility. At minimum however, team members would be required to be assigned to all entry lanes, exit lanes, curbside zones, and staging lots during 24/7 operations. Team members would conduct manual verification of registration through visual observance of permits and decals, and conduct traffic counts. The ALPR – GTMS removes the necessity of staffing for this purpose.
☐	Staff Safety	
X	Data Quality	The ALPR – GTMS technology is verified against the AVI technology to verify that all permitted vehicles' trips have been documented for tracking and fee assessment purposes, in case the AVI malfunctions and fails to read the airport affixed transponder. The ALPR – GTMS is also used in concert with AVI to confirm whether a commercial vehicle on Airport roadways is a permitted operator.
X	Other	The ALPR – GTMS technology enables the Airport to assess trip fees on permitted Commercial ground transportation operators. In 2019, the Airport collected a total of $64,815,649 in trip fees from ground transportation operators.

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. The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Company's registered DBA Permit Type Location of record Date and Time of record	.xml, .pdf, .html, .jpg, .xml	Level 2
Images of license plates	.jpg, .xml	Level 3
Date & time image taken	.jpg, .xml	Level 3

Notification:	The commercial ground transportation operators acknowledge notice of GTMS policies and procedures, which include the Airport's use of ALPR and Electronic Toll Readers, by signing the Airport permit. In addition, in compliance with California Civil Code § 1798.90.5, the Airport shall notify the public of the ALPR – GTMS surveillance technology operation by posting the ALPR – GTMS privacy and usage policy on FLYSFO.

The public notice shall include 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:

Use of the Ground Transportation Management System (GTMS) software is required for data access. Agreement and adherence to the City and County of San Francisco's and Airport's computer and data information systems policies, supervisor approval for use, and GTMS Administrator approval for use. Request for system access is to be submitted through SFO's ITT Help Desk ServiceNow online request form. Access can be limited and varied dependent on software system user role. GTMS Administrator and ITT to determine and provide permissions on user role. Training to be provided once software is installed on computer or laptop.

Data can only be accessed through the permissions-controlled GTMS software. The data is to be used for trip and revenue analysis for internal purposes. Information deemed low risk such as Permit Type i.e. Limousine, Taxi, trip counts may be aggregated and shared with the public, other airports, and transportation industries. The public may request trip and revenue information through a public records request.

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.

- 1825 Principal Administrative Analyst II
- 1823 Senior Administrative Analyst
- 1822 Administrative Analyst
- 7315 Automotive Machinist Assistant Supervisor
- (2) 5290 Transportation Planner IV
- 7381 Automotive Mechanic
- 0931 Manager III, Airport – Landside Operations

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- TransCore
- LP IBI Group, LLC

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 can only be accessed through the permissions-controlled GTMS software. Users must provide unique computer login credentials such as username and password to access the data. Passwords must comply with the City and County of San Francisco cyber security requirements. The following protocols shall be followed to ensure data security:

- All network equipment and servers containing sensitive data are maintained in a secured
- location accessible only to Airport badged, authorized personnel.
- Servers and network equipment are continuously monitored.

- ITT maintains a log of successful and unsuccessful logon attempts, changes in user accounts, whether user logs have been modified, network threats, and resource access.
- All SFO workstations and servers are patched regularly.
- All sensitive data stored on the servers are backed up regularly and a copy saved offsite
- SFO's network is protected behind a firewall and data transmitted outside SFO's network to SFO cloud-based partners are encrypted via SSL/TLS. Data at rest offsite are also encrypted.

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 – GTMS Technology 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.

The Department currently participates in the following sharing practices:

A. Internal and External Data Sharing

- GTMS Users for review of matching license plates and electronic toll reads;
- District Attorney's Office in accordance with the law; and
- Public Defender's Office or criminal defense attorney in accordance with California discovery laws; law enforcement agencies as part of a criminal or administrative investigation; Parties to civil litigation, or other third parties when required under law.

Data sharing occurs at the following frequency:

- On request in accordance with the law, or during SFO presentations on topics related to ground transportation activity.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

X Confirm the purpose of the data sharing aligns with the department's mission.

X Consider alternative methods other than sharing data that can accomplish the same purpose.

X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

X 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.

X Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

B. Department shares the following data with the recipients:

- Aggregated trip counts and revenue by permit types. Data constituting PII or other sensitive information will be shared with law enforcement agencies in accordance with the law, and with parties involved in criminal, civil or administrative proceedings as required under law.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

- Data collected is primarily to be accessed by internal stakeholders within the Airport department. All Airport users are to comply with the Airport's computer and cybersecurity polices, as agreed upon through daily computer sign-in. Data shared with external entities or other City and County departments are to fall within the Level 2 category of non-sensitive data for the business purposes of improved commercial ground transportation and analyses. Information within the Level 3 low-moderate risk category must be requested through the public records request process, and the data is reviewed prior to disclosure to ensure that it is subject to disclosure under the Public Records Act and the Sunshine Ordinance.

- The Department 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.

Data Retention:

The Department's data retention period and justification are as follows:

- Data is active for 18 months in the production server, then 4.5 years in cloud storage.
- Airport server storage size limits retention on production server
- Airport Data Retention Policy requires 4.5 years
- Data would only be retained longer than above if/when the City Attorney issued a litigation hold letter to the Airport.

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
- Cloud Storage Provider

Data Disposal:

Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices: Data is consolidated on the local storage and moved to cloud provider for long term storage. Local drives are overwritten with new data. Cloud storage data is deleted.

Processes and Applications: Not applicable for this technology solution.

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.

In-person or virtual training session that includes system overview and use of reporting modules.)

COMPLIANCE

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

The Airport's Information Technology and Telecommunications (ITT) and Government Affairs & Policy teams will both govern and oversee compliance of the policy. Any resulting policy is to be shared with the Airport community with follow-up items, if any, documented.

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

- Manager of ITT Business Services
- Senior, Landside Transportation Planner

Sanctions for violations of this Policy include the following:

- Airport Commission employees will be disciplined for violation of the Ordinance subject to meeting and conferring with the unions representing Airport Commission employees.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.

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 completing a Contact SFO Form found on FLYSFO.COM. The submissions are reviewed by the Airport Guest Services team and forwarded to the Airport stakeholder team responsible for follow-up, as necessary, on the topic of concern or comment. Additionally, the Airport Commission holds bi-monthly public meetings where the public may register complaints or concerns during the Public Comment section of the calendared agenda.

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

- Include in the daily tasks and job duties of Landside staff and its contractors to respond to complaints and concerns submitted by the commercial transportation.
- Consistent with these duties, Landside staff responds to all inquiries from commercial passenger transportation providers.
- In addition, the Airport's Guest Services team dedicates a staff to address complaints and concerns from the public.
- Any matters brought to the Airport are tracked from initial receipt of communication through closure of follow-up actions, if any.

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.