Surveillance Technology Policy

Application Based Commercial Transport (ABCT)
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 Application Based Commercial Transport (ABCT) technology 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

We provide an exceptional airport in service to our communities.

The Surveillance Technology Policy ("Policy") defines the manner in which the Application Based Commercial Transport (ABCT) technology 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 Application Based Commercial Transport (ABCT) technology, 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 Application Based Commercial Transport (ABCT) technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– *Perform Transportation Network Companies (TNC) invoice reconciliation.*
– *Enforce operating agreements.*
– *Support Public Safety by ensuring only authorized and approved drivers and vehicles are allowed to service passengers at SFO.*
– *Administer and regulate mobility programs.*

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

Departments may use information collected from technology 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

Application Based Commercial Transport (ABCT) technology supports the Department's mission and provides important operational value in the following ways:

It uses location data to enforce operating agreements for regulated mobility programs, administer and regulate these programs, and for general transportation planning.

In addition, Application Based Commercial Transport (ABCT) technology promises to benefit residents in the following ways:

the following ways:

	Benefit	Description
☐	Education	
X	Community Development	Equitable distribution of and access to transportation
☐	Health	
X	Environment	Traffic patterns and congestion within SFO
☐	Criminal Justice	
X	Jobs	TNC companies and driver's; GTU resources
☐	Housing	
X	Public Safety	Reduces risk of fraud and unethical business practices.
☐	Other: Passenger Preference for this type of ground transportation	Passenger Preference for this type of ground transportation

Application Based Commercial Transport (ABCT) technology will benefit the department in the following ways:

	Benefit	Description
X	Financial Savings	Not having to hire additional staff to manually monitor and manage the TNC's activities.
X	Time Savings	Staff can reconcile monthly invoices quickly with the use of aggregated data, saving dozens of hours per month of accounting time.)·

	Staff Safety	
X	Data Quality	Human error is reduced; information is legible and can be easily sorted and summarized by computers & can be paired with analytical analysis; likely reduction in fraudulent handwritten records; increase in the number of records, since they are automatically created and sent
X	Other: Enforcement of non-compliant drivers	Improved enforcement of non-compliance: drivers exceeding curbside staging times, drop-off and pick-ups at non-designated areas.

To achieve its intended purpose, Application Based Commercial Transport (ABCT) (hereinafter referred to as "surveillance technology") works in the following way: Data from TNCs (Transportation Network Companies) is collected by a third-party platform and relayed to SFO in real-time. SFO keeps all the data for historical analysis.

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 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 type(s):

Data Type(s)	*Format(s)*	*Classification*
GPS Location Date	JSON, XML, Relational Database Management System (RDBMS), CSV	Level 2
Enter-ing and Exit-ing of the SFO location's geofence	JSON, XML, Relational Database Management System (RDBMS), CSV	Level 2
Vehicle license plate number	JSON, XML, Relational Database Management System (RDBMS), CSV	Level 2

Note: All the following Data Types are Classified Level 2 - Internal Use based upon the City's Data Classification Standard.

- UID (Unique ID created by concatenation of the anonymized driver IDd and trip ID.)
- TNC ID (a five-digit unique integer assigned to each TNC operating at SFO.)
- License Plate (Seven-character or less, numerical and alphabetic, that represents the vehicle license plate. Accepts an empty String value if there hasn't been a license plate assigned yet.)
- Timestamp (The current time of the event or "ping" expressed in ISO 8601 combined date and time in UTC using 24-hour clock.)
- Transaction Type (The four types of events or "pings" as defined in the national standard in the terms and conditions of the system: "DROP-OFF", "PICK-UP", ENTER", "EXIT".)
- Ride Count (Number of active TNC rides in the vehicle following the transaction event/ping.)
- Longitude (The longitude coordinate in WGS84 of the event or "ping" expressed as a positive or negative number. For locations in North America, this will always be a negative number. This value should have a minimum precision of six decimal places.)
- Latitude (The latitude coordinate in WGS84 of the event or "ping" expressed as a positive or negative number. For locations in North America this will always be a positive number. This value should have a minimum precision of six decimal places.)

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:

X Information on the surveillance technology

☐ Description of the authorized use

X 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):

- The requestor must submit a request to a data steward (within an SFO Business Unit) for the location data. The data steward obtains the user's requirements for data and its format for an authorized use. The data steward confirms end-user authorization and signals technical staff (SFO ITT) to retrieve and send data to the requestor through a secure channel if necessary.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- Airport Planners (5200 series)
- Administrative Analysts (1840; 1842;1844)
- Information Systems Business Analysts (1052;1053;1054)
- Information Systems Engineers (1042;1043;1044)
- Information Systems Project Directors (1070)

B. Members of the public, including criminal defendants

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.

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:

- Technical Safeguards: Secure network, password-protected systems, encryption of data where necessary.
- Physical Safeguards: There are physical access restrictions for each server room containing database systems (i.e., badge access, locked door).

Data Sharing: The Department will endeavor to ensure that other agencies or departments that may receive data collected by the Application Based Commercial Transport (ABCT) Policy will act in conformity with this 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.

The Department 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)

The Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, 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.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their response.

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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Type	Recipient
Raw data for TNC operations at Airport.	City Attorney's Office

Data sharing occurs at the following frequency:

Limited dataset provided upon request. This has occurred less than 10 times in the past year.

B. External Data Sharing

Department shares the following data with the recipients:

Type	Recipient
Raw data for TNC operations at Airport.	TNC's (e.g., Uber, Lyft, etc.)

Data sharing occurs at the following frequency:

As needed for billing and administrative/operational compliance, including fines.

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

The Department does not share raw data unless they are employees, contractors or consultants under contract with a legitimate business need for such data. Data will not be shared externally or publicly, unless legally requested through the Sunshine Ordinance or the CA Public Records Act, or if requested by universities, consultants, or other transportation agencies. All shared information will be aggregated or redacted and only datasets limited to the requestor's request will by provided. As per the Public Domain Dedication and License (PDDL), public data is provided for on an "as is" basis and for informational purposes only. The Department and City make no warranty, representation, or guaranty of any type as to the completeness, accuracy, content, or fitness for any particular purpose or use of any public data set made available nor shall any warranties be implied with respect to the data provided. The Department and City ask that recipients of publicly released data follow the Terms of Use published on DataSF's website.

Before data sharing with any recipient, 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 Evaluate 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	**Retention Justification**
SFO keeps data according to the retention policies established by the Department and approved by the Airport Commission (i.e.,Executive Directive 18-05) as well as, applicable legislation. When multiple retention standards apply, SFO utilizes the most restrictive legislation for each class of data. Permittees and vendors are required to retain data for the time period specified by legislation and permit conditions. Retention time periods vary by mobility program.	All data will be retained for transportation planning purposes, enforcement of operating agreements, regulation of mobility programs, and to ensure equitable distribution of transportation options throughout 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):

- Location data that is used for prosecutorial or investigatory purposes will be retained beyond the stipulated retention period(s). Location data may also be retained for analytical purposes related to aforementioned authorized use cases, including but not limited to, the assessment of trends.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

X Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)

☐ Department of Technology Data Center

X Software as a Service Product

X Cloud Storage Provider

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

Practices:

- Local data stores are wiped when computers are turned in.

Processes and Applications:

- Not applicable.

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.

Training is provided on an as-needed basis due to the low number of staff who have authorized access to such location data, the specialized software needed, the specialized job skills needed to retrieve and analyze such data, and the business requirements for their roles.

COMPLIANCE

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

Currently any changes in these data sets or technical routines that manages this system are controlled through our Change Management Process and documented as such. All access is requested through a formal request and approved by the data stewards. Prior to accessing the data, all authorized staff shall be required to review and agree to Department's Surveillance Technology Policy. Access is role based controlled – access is only provided once approved. At any time, ITT can see who has / who had access to a specific dataset. .

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

- SFO Legal Staff (8181-83)
- Chief Information Office (0951-54)
- ITT Business Services Manager (0941-43)
- SFO Business Unit Managers (0922-23; 0931-33 & 0941-43)

Sanctions for violations of this Policy include the following:

The discipline processes are established in the various Memoranda of Understanding (MOUs) that apply to the different classifications of employees represented by the corresponding unions.

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 <u>not</u> 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:

Members of the public can access www.flysfo.com to register complaints or concerns or submit questions via the "Contact Us" web page and form.

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

SFO uses ZenDesk to collect and route inquiries to the appropriate department at SFO.

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.