Surveillance Technology Policy

Tenant Security Cameras
SAN FRANCISCO INTERNATIONAL AIRPORT ("SFO", "Airport", OR "Department")

The City and County of San Francisco values the privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, this Surveillance Technology Policy aims to ensure the responsible use of Security Camera Systems by airlines, concessionaires, food and beverage operators, rental car agency tenants (hereinafter Tenants) at the San Francisco Internal Airport ("SFO", "Airport", OR "Department") as well as any associated data to which Department is privy, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

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

The Surveillance Technology Policy ("Policy") defines the manner in which the Tenant Security Camera System (fixed or mobile) will be used to support Department operations.

This Policy applies to all Department personnel, and other agents acting on the Department's behalf that access or use digital recordings or other data from Tenants Security Camera Systems, including employees, contractors, and volunteers.

POLICY STATEMENT

This policy applies to the Airport's access to and use of digital recordings and other data from the security cameras of the following entities:

- Airport Tenants

The Airport limits its use of recordings and other data from Tenant security cameras to the following authorized use cases and requirements listed in this Policy only.

Authorized Use(s):

1. Reviewing camera footage in the event of an incident.
2. Approving Tenant's disclosure of digital recordings and other data from its security camera system.

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

Department's processing of personal data revealing legally protected categories, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Surveillance Oversight Review Dates
COIT Review: February 17, 2022
Board of Supervisors Review: Upcoming

BUSINESS JUSTIFICATION

Access to and use of digital recordings and other data from Tenant Security cameras will benefit the Department in the following ways.:

	▪ Education	
	▪ Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
	▪ Environment	
X	Criminal Justice	Review video footage after a security incident.
	▪ Jobs	
	▪ Housing	

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Equipment is owned and operated by non-city entity.
X	Time Savings	Tenant/Contractor Security Camera Systems operate 24/7/365, thus decreasing or eliminating building or patrol officer supervision. Additionally, full-time staffing is not required to subsequently review footage of security incidents.
X	Staff Safety	Tenant/Contractor Security cameras help identify violations of Building Rules and Regulations, and City, State and Federal law and provide assurance that staff safety is emphasized and will be protected at their place of employment.

- Service Levels

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.

Data Collection:

Department shall only collect the data that is necessary to execute the authorized use cases. All surveillance technology data shared with Department by a Tenant/Contractor, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects some or all of the following data types:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 3
Date and Time	MP4 or other format	Level 3
Geolocation data	TXT, CSV, DOCX	Level 3

Access:

The Airport does not have direct system access to, or control over, the operation of Tenant's technology. Recorded footage is accessed only in response to an incident.

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:

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0931 – Manager Aviation Security & Regulatory Compliance.
- 0933 - Director, Security, Emergency Management & Communications
- 0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

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

- Tenants/Vendors are responsible for the maintenance of the surveillance technology systems.

B. Members of the public

	Data collected by surveillance technology will not be made generally available to members of the public. 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. 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 Members of the public 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 any PII received from Tenant (or shared by Tenant) 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) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the Department. Departments shall, at minimum, apply the following safeguards to protect surveillance technology information received from Tenant from unauthorized access and control, including misuse: - Encryption: Data retained by the Department will be encrypted. Raw data may be retained by the Department only for the authorized use case of sharing with law enforcement or the public. - Storage: Any use of a third-party service provider must meet City's cyber security requirements. - Audits: A data access log will be maintained by the Department for all Security Camera data that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, department requesting data, date/time of access of raw data, outcome of data processing, as well as, date processed data was delivered to users.
Data Sharing:	Tenant/Contractor is the sole owner and custodian of its Surveillance Technology data. Tenant/Contractor may share such data with the Department, but pursuant

to Airport Rule & Regulation 7.5, must seek prior authorization from Department for release to other third parties.

The Department will endeavor to ensure that other agencies or departments that may receive data collected by Tenant's security cameras will act in conformity with this Surveillance Technology Policy.

In the event of a substantive amendment to Rule 7.5, the Department must resubmit this Policy for approval in accordance with Chapter 19B.

Data is shared by Tenant/Contractor with the Department as needed.

A. Internal Data Sharing

In the event of an incident, Security Camera images may be shared with the following agencies:

- Within the Department on a need-to-know basis
- Police
- City Attorney
- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other law enforcement agencies
- Member(s) of the public, if required under the California Public Records Act or the Sunshine Ordinance

Data sharing occurs at the following frequency:

- As needed.

Data Retention:	Department may store and retain PII data shared by Tenant/Contractor only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the Department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections. The Department's data retention period and justification are as follows: - One year, consistent with the Department's Data Retention Policy and state law; longer if necessary for an ongoing investigation or in anticipation of litigation. 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): - If necessary for an ongoing investigation or in anticipation of litigation. Data may 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 ▪ 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: - Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.
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 on behalf of Department must receive training on data security policies and procedures. - Annual cybersecurity training (COIT Policy Link)

COMPLIANCE

Department shall oversee and enforce compliance with this Policy according to the memoranda of understanding with the labor organization representing employees of the City and County of San Francisco.

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.

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

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0931 – Manager Aviation Security & Regulatory Compliance.

- 0933 - Director, Security, Emergency Management & Communications
- 0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

DEFINITIONS	
Tenant/Contractor	Non-City Entity that owns and operates security cameras and shares security camera footage with a City department.
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.

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, concerns or questions can be submitted to:

- *Airport Guest Services - https://www.flysfo.com/contact-sfo(Contact SFO)*
- *Airport public email, phone, or website --https://www.flysfo.com/contact-sfo or*
- *Airport Commission meetings -- https://www.flysfo.com/about-sfo/airport-commission/addressing-the-commission*

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall follow its process where questions and complaints are tracked by Airport Guest Services and response are promptly responded to by the Director of Guest Experience and/or his staff.

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.

Attachment 1: Appendix A: Rules and Regulations, Rule 7.5 (2022 edition)

RULE 7.0

AIRPORT SECURITY

7.5 VIDEO MONITORING AND RECORDING DEVICES / ACCESS TO AIRPORT CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM

(A) Installation or Removal of Video Monitoring and Other Recording Devices

No video monitoring or other recording devices may be installed or removed by any Airport tenant or contractor in or around the Airport premises without prior written authorization from the Aviation Security unit. To obtain authorization for CCTV camera installation or removal, tenants and contractors must submit an application, specifying the following:

- Field-of View (FOV) screenshots
- Video monitoring/recording device model and specifications
- Recording system and retention time
- Camera layout drawing
- Security infrastructure and plan to prevent unauthorized access

The use of Pan-Tilt-Zoom (PTZ) security cameras by tenants and contractors in any Restricted area is strictly prohibited and no video monitoring and/or recording device may be installed or focused in a manner that depicts/records security checkpoints, or doors that provide access to any area on Airport premises that, in the sole and exclusive discretion of the Director or his designee, is deemed to present a potential risk to Airport security. All subsequent changes or modifications to tenant and contractor video monitoring and/or recording device use must be submitted to Aviation Security in writing and approved prior to executing modifications.

(B) Remote Viewing and Authorization Access

No video monitoring and/or recording device data may be streamed or otherwise transmitted on a wireless network unless the wireless network is equipped with WPA2 security. Real-time access to all footage must be available to the Aviation Security unit at all times. No tenant or contractor shall release any video monitoring and/or recording device footage from cameras/devices without prior written authorization from the Aviation Security unit and, if deemed appropriate, the TSA. Remote access to video monitoring and/or recording devices in secure areas will not be permitted unless explicitly authorized by the Director.

All forms of video footage, whether real-time or stored, must be password protected. Passwords must comply with the Airport's Password policy.

(C) Inventory of Video Monitoring and Other Recording Devices

All tenants and contractors shall provide Aviation Security with an inventory of existing video monitoring and/or recording devices and security plans, including all of the following:

- Device manufacturer, model and specifications
- Field-of-view
- Data retention time
- Placement of video monitoring and/or recording devices

- Remote access usage
- Written security plan detailing how unauthorized access will be prevented

(C) Airport Closed-Circuit Television (CCTV) Access Policy

The Airport owns and operates the CCTV system. This system contains information that is confidential, which may be sensitive secure, affect personal privacy, or both. A tenant or contractor may access Airport CCTV feeds only through Airport equipment upon request to Airport Aviation Security (AVSEC). If access is granted, the tenant or contractor shall designate individual employees to view CCTV feeds for the performance of official job duties, on a need-to-know basis only. Any such individual must hold an Airport ID badge and execute a Non-Disclosure Acknowledgement as a condition of authorized access. (ASB 20-02, ASB 20-06)