Surveillance Technology Policy

Security Cameras
San Francisco International 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 the Department's Security Camera System (hereinafter referred to as "surveillance 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 Surveillance Technology Policy ("Policy") defines the manner in which the Security Camera Systems (fixed or mobile) will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all department personnel that use, plan to use, or plan to secure the surveillance technology 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 the surveillance 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.	Live monitoring.
2.	Recording of video and images.
3.	Reviewing camera footage in the event of an incident.
4.	Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

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

Department 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.

All data collected by surveillance cameras is the exclusive property of the City and County of San Francisco. Under no circumstance shall collected data be sold to another entity.

Surveillance Oversight Review Dates
PSAB Review: 1/25/2024, Recommended: 1/25/2024
COIT Review: 2/15/2024
Board of Supervisors Approval: TBD

BUSINESS JUSTIFICATION

Reason for Technology Use

The surveillance technology supports the Department's mission and provides important operational value in the following ways:

See Appendix A Below.

Description of Technology

See Appendix A Below.

Resident Benefits

The surveillance technology promises to benefit residents in the following ways:

	Benefit	Description
▪	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; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
▪	Jobs	
▪	Housing	
X	Other	Better management of city assets by leveraging remote condition assessment. Improvement of overall Situation Awareness.

Department Benefits

The surveillance technology will benefit the department in the following ways:

	Benefit	Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus decreasing or eliminating building or patrol officer supervision.

X	Staff Safety	Security cameras help identify violations of the City Employee's Code of Conduct, 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.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Other	Security cameras will enhance effectiveness of incident response and result in improved level of service.

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.

Data Collection: Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects some or all of the following data type(s):

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

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas in accordance with Section 19.5 of the Administrative Code. 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
X Description of the authorized use
- Type of data collected
- Data retention

X Department identification
X Contact information

Access: All parties requesting access must adhere to the following rules and processes:

Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.

Access to live views and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident.

Details on department staff and specific access are available in Appendix A.

1. ***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:

See Appendix A Below.

2. ***Members of the public***

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. 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.

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.

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 dictated by this policy. 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.

More specifically, Department training will include:

Annual cybersecurity training (COIT Policy Link).

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) 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.

Department shall ensure compliance with these security standards through the following:

- 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 the 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 Storage: 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.)

X Department of Technology Data Center

X Software as a Service Product

X Cloud Storage Provider

Data Sharing: Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology 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.

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)*

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

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 legal obligations.

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 and ensure all PII is removed in accordance with the department's data policies. NOTE: The Airport's camera software currently does not have the capability to "scrub faces" and Facial Recognition Technology is not used.
- 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Department may share Security Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Security Camera images may be live-streamed or shared by alternative methods to the following agencies within the City and County of San Francisco:

Data Type	Data Recipient
Video and Images Date and Time	- Within the operating Department - Police - City Attorney - District Attorney - Sheriff - On request following an incident.

Frequency - Data sharing occurs at the following frequency:
- As needed.

B. External Data Sharing:

The department shares the following data with recipients external to the City and County of San Francisco:

Data Type	Data Recipient
Video and Images Date and Time	Other local law enforcement agencies Airport Tenants, Contractors and Sub-Contractors

NOTE: Tenants, Contractors and Sub-Contractors are required to adhere to the Airport's requirements for protecting and maintaining video data via the contract Terms with the Airport.

Frequency - Data sharing occurs at the following frequency:
- As needed.

Data Retention: Department may store and retain raw PII data 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:

Retention Period	Retention Justification
1. Security Camera data will be stored for one (1) year to be available to authorized staff for operational necessity and ready reference.	This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

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.

Exceptions to Retention Period - PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

If data is associated with an incident, it may be kept for longer than the standard retention period.

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

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

1. Automatic overwrite of all existing files when the standard data retention period ends.
2. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.

COMPLIANCE

Department Compliance

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

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.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

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

See Appendix A Below.

Oversight Personnel

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

See Appendix A Below.

Sanctions for Violations

Sanctions for violations of this Policy include the following:

See Appendix A Below.

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 Inquiries

See Appendix A Below.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

See Appendix A Below.

Inquiries from 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: Department Specific Responses

Department: San Francisco International Airport

1. **Reason for Technology Use**

The surveillance technology supports the Department's mission and provides important operational value in the following ways:

The technology helps to protect and provide for the Safety and Security of our passengers, the public, and all Airport employees.

2. **Description of Technology**

A. Airport Cameras

The Airport uses Verint Video Management Software (VMS) and, primarily, Pelco Analog and Digital Pan-Tilt-Zoom (PTZ) and fixed cameras. The cameras are installed in public areas of the Airport. Specific to this submission, the cameras are located pre-security.

The Verint system is a closed system, running on a security local area network that is not exposed to the Internet.

B. AirTrain and SFO Shuttle Buses

The closed-circuit television (CCTV) system security cameras on the AirTrain vehicles and the SFO Shuttle Buses captures and records video images of passengers. The CCTV security cameras and the images/video they capture shall be used for business purposes only and not for personal use. The security cameras shall be used 24 hours a day, 365 days per year.

For the AirTrain vehicles, each vehicle has four Safe Fleet VMAX cameras mounted to the ceiling to provide video of the interior to an onboard Digital Video Recorder (DVR) which is also located inside the vehicle. The cameras record when the train is fully powered. The DVR has a microSD card that stores video recordings for two-weeks and automatically rewrites after that time. For viewing, the microSD card is removed with a key by AirTrain Administration personnel only and can be viewed on a password protected computer.

Each SFO Shuttle bus is equipped with multiple video cameras capturing multiple interior and exterior views. Interior cameras also capture sound. The footage is stored in an onboard DVR device located in a locked cabinet. The DVRs overwrite footage every 30 days. The only way to preserve footage is to remove the DVR, connect it to a

secured computer in the Administrative Office, and save the images to this password protected computer.

C. BART CCTV System and Video Streaming

The BART CCTV system will provide video streaming from 50 cameras deployed around the Airport BART Station to seven Airport workstations primarily at the Airport's Security Operations Center (SOC) using the VIDSYS Software Platform.

The VIDSYS Software Platform:

The Vidsys CSIM software platform continuously fuses, instantly correlates, and converts vast amounts of data into meaningful and actionable information gathered from virtually any type, brand, or generation of physical security system or sensor, and from many other networked management applications. The automated tools support safe, effective, and timely resolution of incidents and alarms. The tools also manage complex incidents that involve multiple simultaneous alarms at one or more locations.

The Vidsys CSIM platform has two primary components: Situation Awareness and Situation Management. The platform comes with software applications that integrate each category of devices with the single operating platform. As a secure web-based solution, the Vidsys platform allows operators to manage assets for a single facility or multiple locations.

3. **Access to the Technology and Department Compliance**

The specific categories and titles of individuals who are authorized by the Department to access or use the collected information:

- 9202 - 911 Dispatcher
- 9203 - 911 Dispatch Supervisor
- 9212 - Security Operations Center (SOC) Analyst
- 9213 - Airfield Safety Officer
- 9220 - SOC Supervisor
- 9221 - Airport Operations Supervisor

  5290 – Senior Transportation Planner
- Air Train Staff and Contractors
- Aviation Security System MX Contractors

- Ground Transportation Unit (GTU)
- Parking Management
- SFPD-AB
- San Mateo County Sheriff and District Attorney

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

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

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

The Department will endeavor to ensure that other agencies or departments that may receive data collected by Airport cameras, AirTrain cameras, SFO Shuttle Bus cameras, and BART's security cameras will act in conformity with this Surveillance Technology Policy.

Oversight Personnel

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

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0923 – AirTrain Safety and Security Manager
- 0931 – Manager Aviation Security & Regulatory Compliance
- 0933 - Director, Security, Emergency Management & Communications and AirTrain Director
  0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

3. **Sanctions for Violations**

Sanctions for violations of this Policy include the following:

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

4. **Public Inquiries**

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.

Public question and complaint can be submitted via the:

- Airport Guest Services (Contact SFO – https://www.flysfo.com/contact-sfo)
- Airport public email, phone, or website (Contact SFO), or
- Airport Commission meetings (How to Address the Commission)

Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

Data is stored on a local server for 45 days, then video files are transferred to Amazon Web Services for up to 1 year. Files are deleted after 320 days based on the lifecycle policy in AWS. BART is the custodian of their video footage, and as such, is solely responsible for the management, retention and destruction of that video footage.

For AirTrain, in accordance with the SFO Executive Directive (ED 18-05) Record Retention and Destruction Policy, video data will be stored in the vehicle for a two-week period before the data is overwritten. Any AirTrain saved images or videos will be retained for 4.5 years. As noted above, the SFO Shuttle Bus footage is stored in an onboard DVR device and is overwritten every 30 days. No Private Personal Information (PII) is stored on the drives. Additional information included with the images and video is the location, vehicle, and time/date.

Is a subpoena required before sharing with law enforcement?

- No