Surveillance Technology Policy

San Francisco International Airport
Gunshot Detection Solution

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, the Surveillance Technology Policy aims to ensure the responsible use of the Department's gunshot detection solution itself, as well as any associated data, and the protection of members of the public who visit the Airport and all those who work at the Airport.

PURPOSE AND SCOPE

The Surveillance Technology Policy ("Policy") defines the manner in which the gunshot detection solution will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure the gunshot detection solution, 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 Airport will limit its use of the gunshot detection solution to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Record the sound of gun shots, aggressive voices, glass breaking, and unusual disturbances (based upon decibel level) and use of device sensors to locate the origin of the sounds.
2. Trigger the Airport's security camera system to record video and images of the specific location where the soundsare occuring.
3. Review of video recordings triggered by the sound of a gunshot, aggressive voices, glass breaking, and unusual disturbance incidents.
4. Provide video footage/images to law enforcement or other authorized persons in connection with the investigation of an incident, or to members of the public when the footage is subject to disclosure pursuant to a Public Records Act request.

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

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.

BUSINESS JUSTIFICATION

The gunshot detection solution supports the Airport's Core Value of "Safety and Security is our first priority" and provides important operational value in the following ways:

The gunshot detection solution is an alert system designed to provide immediate notice and information regarding incidents that potentially threaten the public safety, such as an indoor active shooter incident, aggression, glassbreak or unusual disturbances. As a result, first responders arrive on scene faster, equipped with the vital information needed to contain threats and mitigate casualties. The gunshot detection solution provides immediate and accurate response for Airport Commission staff and law enforcement teams.

In support of Department operations, the gunshot detection solution promises to help with:

☐	Education	
☐	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
☐	Environment	
X	Criminal Justice	SFPD-AB can be quickly alerted and respond, when needed, to the sound of gunshots, aggressive voices, glass shattering, or other high decibel level sound disturbances such as blasts, with improved geographic precision. Video recordings triggered by the detection of these sounds can be provided to law enforcement to assist in its investigation of an incident.
☐	Jobs	
☐	Housing	
X	Other	Improved protection of the public and city assets by leveraging remote condition assessment technology, which improves the overall situational awareness. The technology helps ensure the safety of the 49,000+ people who work at the Airport and the 58 million people (pre-COVID) who fly to and from SFO every year.

In addition, the following benefits are obtained:

Benefit	Description
Financial Savings	The gunshot detection solution, in conjunction with the Airport Security Camera Systems will run 24/7, thus decreasing or eliminating the need for additional building or patrol officer supervision.

X	Time Savings	Airport CCTV cameras provides real-time feeds that run 24/7, thus eliminating lengthy physical surveillance of Airport facilities. Video shall be used to verify the accuracy of written reports regarding the incident.
X	Staff Safety	The gunshot detection solution will provide immediate information about the location of potential threats to staff safety. The gunshot detection solution integrated with the Security cameras provide an immediate view of an incident as it is occurring to better prepare those responding to the incident.
X	Data Quality	The CCTV cameras data resolution can be set by level and is currently set to high resolution.
X	Service Levels	The gunshot detection solution 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 be consistent with all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the gunshot detection solution surveillance technology must be kept 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 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
	Data Class: **Level 3 =** Sensitive	**Description:** 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.	**Potential Adverse Impact:** Low - Moderate

Notification:

The notice requirements in Administrative Code Section 19.5 do not apply to the Airport.

However, the Airport will publish a public notice on its external website at www.flysfo.com regarding the use of this surveillance technology.

The Department's public notice will include the following items:

- 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:

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.

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.

Departments shall, at minimum, apply the following safeguards to protect surveillance technology information 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 shared with a third party. This log will include, but is not limited to, the following: date/time

data was originally obtained/collected, department requesting data, date/time of access of raw data, outcome of data processing, as well as, the date processed data was delivered to users.

Data Sharing:

The Department will endeavor to ensure that other City agencies or departments that may receive data collected by their own Security Camera Systems will act in conformity with this Surveillance Technology 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.

Before sharing data with any recipients, the Department will use the following procedure to ensure doing so is consistent with the policy:

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	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 members of the public.
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, the California Public Records Act, and the various federal, state and local laws protecting privacy.
X	Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and the federal, state, and local laws protecting an individual's right to privacy..

The Department may share Security Camera footage and data from the Gunshot Detection System with the following entities:

A. Internal Data Sharing:

In the event of an incident, Security Camera images and data from the Gunshot Detection System may be live-streamed or shared by alternative methods to the following agencies:

- Within the Airport
- Police
- City Attorney

- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

Department shares the following data with the recipients:

- with outside law enforcement agencies to the extent data is needed to assist in an investigation.
- with the public, to the extent the data is subject to disclosure pursuant to a Public Records Act request.

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 manages its 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:

- Security Camera data will be stored for a minimum of one (1) year to be available to authorized staff for operational necessity and ready reference, subject to technical limitations.

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

- Justification: Per the Airport's Record Retention and Data Destruction Policy (ED 18-05) and the statutes referenced within, which is in compliance with State law, requiring security camera footage be retained for one year. 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.

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.)

X 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: - 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 must receive training on data security policies and procedures. - Annual cybersecurity training (COIT Policy Link)

COMPLIANCE

Department shall oversee and enforce employee compliance with this Policy in accordance with the Memoranda of Understanding of the labor organization representing employee.

If the Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, and the Department determines a violation has occurred, it 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.

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.

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."

Appendix A: Department Specific Responses

1. A description of the product, including vendor and general location of technology.

   The AmberBox gunshot detection solution is a detection and response system designed to protect lives in an indoor active shooter, aggressive behavior, glassbreak and unusual disturbance incidents. By automating the emergency process, first responders arrive on scene faster, equipped with the vital information needed to contain threats and mitigate casualties. The AmberBox gunshot detection solution provides immediate and accurate response for internal and law enforcement teams.

   The AmberBox gunshot detection solution offers the most advanced sensing system available, ensuring maximum protection from threats. Shots are detected through percussion and infrared sensors, that analyze the binodal signature of a gunshot. Combined with AmberBox's gunshot detection solution's algorithm, false alarm sources are virtually eradicated. All analysis is conducted at the sensor (detector), with no real-time audio transmitted, ensuring privacy.

   The Proof of Concept, Phase I, will require the deployment of 25 sensors in the Consolidated Airport Campus Building 674. The sensors will be connected to the Aruba Wi-Fi system for power on the 1st floor (lobby area), as well as, throughout the 4th floor. In Phase II, the sensors will be deployed both pre- and post-security throughout the terminals, as well as, the Airport buildings throughout the campus.

   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.

2. 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*

3. 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 questions and complaints can be submitted via the:

- *Airport Guest Services (Contact SFO)*
- *Airport public email, phone, or website ((Contact SFO), or*
- *Airport Commission meetings (How to Address the Commission)*

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

   Data is in a local server for 45 days; then video files are transferred to Amazon Web Services (AWS) for up to one year. Files are deleted after 320 days based on the lifecycle policy in AWS.

5. Is a subpoena required before sharing with law enforcement?

   - No