Surveillance Technology Policy

Weapons Detection System
Public Health

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 Weapons Detection 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 Department's mission is to protect and promote the health of all San Franciscans. SFDPH strives to achieve its mission through the work of two main Divisions - the San Francisco Health Network and Population Health.

The Surveillance Technology Policy ("Policy") defines the manner in which the surveillance technology 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. Review real-time photo after an object has been detected, that will need further screening.
2. Review real-time photo that identifies the area on a person or an item being carried, where a possible weapon threat is located.

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.

BUSINESS JUSTIFICATION

Reason for Technology Use

Surveillance Oversight Review Dates
PSAB Review: TBD (list all dates at PSAB, and write "Recommended: MM/DD/202X" for rec date)
COIT Review: TBD (list all dates at COIT, and write "Recommended: MM/DD/202X" for rec date)
Board of Supervisors Approval: TBD

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

The concealed weapons detection system is designed to enhance physical security in high-traffic public venues by combining advanced sensor technology real-time computing, and machine learning to accurately detect threats.

Description of Technology

The weapons detection sensor uses machine learning models to detect weapon signatures from sensor information gathered from visitors in real time. The sensory information gathered here refers to electromagnetic sensors and visual cameras. Weapon signatures and images collected on site are referred to as 'scan data.' The scan data collected from visitors to identify the presence of weapon(s) carried on their person.

Resident Benefits

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

	Benefit	Description
☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
☒	Criminal Justice	This technology provides immediate response to possible weapons carried by an individual entering site. System analyses the density of objects that are passed through system.
☐	Jobs	
☐	Housing	
☒	Public Safety	The weapons detection machine prevents, minimizes, and stops crime before being committed.

Department Benefits

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

	Benefit	Description
☐	Financial Savings	
☐	Time Savings	
☒	Staff Safety	This technology detects weapons detected prior to entering facilities.
☐	Data Quality	
☐	Other	

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): Sensor measurements, images, Building 005, 025, and 80/90, GPS coordinates - Format(s): Numerical, CSV, JSON, XML, TEXT, - Classification(s): Measurements from electromagnetic temperature, humidity, and tilt sensors. Images of individuals who walk through the Express towers The physical location of the Weapons machine installation. Vendor provides service personnel enter this at the time of installation. This will help in servicing weapons machine in case an onsite visit is required The GPS location of the weapons machines helps in servicing unit in case an onsite visit is required.

Data Type(s)	Format(s)	Classification
Sensor Measurements	PDF, JPEG, CSV, XML, TEXT	Level 3
Images	PDF, JPEG, CSV, XML, TEXT	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. 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:

- ☐ Information on the surveillance technology
- ☒ Description of the authorized use
- ☐ Type of data collected
- ☐ Data retention
- ☐ Department identification
- ☐ Contact information
- ☐ Persons individually identified

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

- If law enforcement needs information from the technology, the request will go to the DPH Director of Security. The Director of Security then reaches out to the Security Maintenance Planner, who then reached out to vendor tech support to obtain the needed information.

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:

- 7262 Maintenance Planner (2)
- 0953 Deputy Director III (1)

B. 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:

Sheriff's staff members were trained by installer technicians how to start up, shut down, operate and test with mock items to be detected.

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 frameworks selected by the department.

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

Administrative Safeguards: Users designated as Admins can select one of the following options:

- Results Only (Default): Alerts and images of all people passing through Express are stored. Scan data are not stored.
- None: No scan data, alerts, or images are stored on disk. Scan data, alerts, and images are only stored in the computer's memory until the alert is dismissed by the tablet operator.

Data is limited to those authorized to review data and cyber security-related technology .

Technical Safeguards: Data stored on the Express computer's disk is automatically deleted after 30 days or sooner if the disk fills up, and room needs to be made for newer data.

Physical Safeguards: Limited admin access to select few to change any options. Tablets are removed from the area and placed in a secured cabinet when not in use.

Data Storage: Data will be stored in the following location:

- ☒ 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
- ☐ 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, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- 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.

A. Internal Data Sharing:

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

Data Type	Data Recipient
Photo image of individual can be provided for investigations	Police Department, Sheriff's Department, City Attorney's Office

Frequency - Data sharing occurs at the following frequency:
Information is shared when there is a legal investigation that necessitates information.

B. External Data Sharing:

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

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

Weapons detection machine does not maintain any photo past a 24-hour time period. Any information needed will need to be formally requested to/from the vendor.	During investigations, litigations there may be a need to request from vendor. Otherwise, weapons detection does not retain images longer than 24hrs.

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):

- Data can be retained due to investigations and litigations that require for information to be held for court proceedings.

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:

- Practices: All Department of Public Health vendor contracts specify NIST data destruction recommendations and standards. Any site that uses weapons detection will not have photo images after machine is turned of at the end of the day. Images are deleted at the end of the day, unless needed for investigations or litigation. In that case, the Department will reach out to the vendor for information.
- Processes and Applications: Weapons detection does not retain any photo images after unit is turned off.

COMPLIANCE

Department Compliance

Department shall oversee and enforce compliance with this Policy using the following methods: In line with the DPH Compliance Policy, the Office of Compliance and Privacy Affairs (OCPA) runs a program that helps prevent and address healthcare fraud, waste, and abuse. This includes looking into reports of possible violations and reviewing areas that may pose risks.

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:
Data stored on the weapons detection disk is automatically deleted at the end of 24 hours. Any information needed will need to be formally requested from vendor.

Oversight Personnel

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

- 0953 Deputy Director III (DPH Director of Security)

Sanctions for Violations

Sanctions for violations of this Policy include the following:
In line with the Department of Public Health Compliance Policy: Operation of a Compliance Program, department aims to ensure that all staff follow our standards and applicable laws. When someone falls short of these expectations, the Department will work to recommend appropriate discipline or corrective action - up to and including dismissal if necessary.

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 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

The public can contact the Office of Patient Experience 6 at:

- Address: 1001 Potrero Avenue, Building 25, Room H1246, San Francisco CA 94110
- Phone: 628-206-5176
- Email: dph-patientexperience@sfdph.org

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

The Patient Experience Department will forward the public's complaint/concern to the personnel assigned to oversee Surveillance Technology Policy to conduct an investigation of the occurrence and provide the complainant with a response of the outcome within 30 business days.

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.