Surveillance Technology Policy

Tenant/Contractor Security Cameras

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 [Third Party name] (hereinafter Tenant/Contractor) Security Camera System by 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 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 that use, plan to use, or plan to secure Tenant/Contractor Security Camera Systems or data, 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

City departments using this policy will limit their use of Tenant Security Camera to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring.
2. Reviewing camera footage in the event of an incident.

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.

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras promise 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	Review video footage after a security incident;
☐	Jobs	
☐	Housing	
X	Other	Better management of city assets by leveraging remote condition assessment. Improvement of overall situational awareness.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Tenant/Contractor Security Camera Systems will save on building or patrol officers.
X	Time Savings	Tenant/Contractor Security Camera Systems will run 24/7, thus decreasing or eliminating building or patrol officer supervision
X	Staff Safety	Tenant/Contractor Security cameras help identify violations of 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		
X	Service Levels	Tenant/Contractor 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.

Data Collection:	Department shall only collect data required to execute the authorized use case. All surveillance technology data shared with Department by 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

Notification:	Departments shall notify the public of Tenant/Contractor surveillance technology operation at the site of operations through signage in readily viewable public areas in accordance to Section 19.5 of the Administrative Code. Department notifications shall identify the type of technology being used and the purpose for such collection. The Department's public notice will include the following items: X Information on the surveillance technology ☐ Type of data collected ☐ Will persons be individually identified ☐ Data retention
Access:	Prior to accessing or using data, authorized individuals within the Department 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 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 may be retained by the Department only for the authorized use case of reviewing camera footage in the event of an incident.
- 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, other than live views, received from Tenant/Contractor 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 (if any), date/time of access of 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 or other entities solely at its discretion. Data is shared by Tenant/Contractor with the Department on the following schedule: ☐ As needed ☐ Weekly ☐ Monthly ☐ Other: -
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:

- Security Camera data shared with Department by Tenant/Contractor will be stored only for the period necessary for investigation or litigation following an incident.

- Justification: This retention period safeguards PII from inappropriate or unauthorized use by minimizing the period and purposes for which it may be retained.

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: - 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 respective memorandum of understanding of employees and their respective labor union agreement.

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.

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.

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

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.

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