Surveillance Technology Policy

Non-City Entity Surveillance Cameras
San Francisco Police Department (SFPD)

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 "Non-City Entity" 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 Department's mission is to protect life and property, prevent crime and reduce the fear of crime by providing service with understanding, response with compassion, performance with integrity and law enforcement with vision.

The Surveillance Technology Policy ("Policy") defines the way the non-city entity Security Camera System will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure non-city entity 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

This policy applies to security camera data sharing between SFPD and the following entities:

- Any non-City entity or individual, through consent, subpoena or search warrant who regularly provides SFPD with data access or information acquired through the entity's or individual's use of surveillance cameras or surveillance camera networks owned, leased, managed and/or operated by the entity or individual. These entities do not have financial agreements with SFPD.

This policy excludes any surveillance cameras that meet both of the following conditions:

- Paid for through a city grant
- Owned by a non-City entity that is under a contractual agreement with the City requiring them to share live feed or historical footage from the camera

SFPD is limited to the following authorized use cases and requirements listed in this Policy only.

Authorized Use(s):

1. Temporary live monitoring during active criminal investigations and significant events with public safety concerns. Temporary live monitoring will cease within 24 hours after the request to the non-city entity is approved and the non-city entity has provided access to

SFPD. SFPD does not record live monitoring.

2. Reviewing specific historical video footage to aid a criminal or internal investigation.

Prohibitions:

- Surveillance camera footage will not on its own identify an individual, confirm racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or information concerning an individual person's sex life or sexual orientation.

- SFPD is prohibited from using data provided by biometric identification or facial recognition technology.

- SFPD is prohibited from live monitoring inside residential dwellings where homeowners/renters have a reasonable expectation of privacy unless one the following conditions exist, exigency per SF Admin Code 19b.7; a homeowner/renter/individual with legal authority to consent, consents, or a warrant is issued.

- SFPD is prohibited from monitoring any certain groups or individuals based solely on race, gender, religion, or sexual orientation. Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action.

- SFPD is prohibited from accessing or requesting surveillance camera live feed during First Amendment activities for reasons outside of redeployment needs due to crowd sizes or other issues creating public safety hazards.

- SFPD members shall not acquire or use surveillance camera footage in cooperation with or assisting U.S. Immigration and Customs Enforcement or Customs and Border Protection in any investigation, detention, or arrest procedures, public or clandestine, where in any such instance the sole, express, or implied purpose is the enforcement of federal immigration laws. SFPD complies with SF Administrative Code Chapters 12H "Immigration Status" and 12I "Civil Immigration Detainers" and SFPD General Order (DGO) 5.15 "Enforcement of Immigration Laws".

BUSINESS JUSTIFICATION

[A description of the product, including vendor and general location of technology]

Categories: Residential, Small Business, Commercial Security Camera Systems.

Subcategories: Indoor, Outdoor

Typical Camera Types [Not vendor specific]:

- Box Camera: A Box Style camera is a standalone camera. The name is derived from the shape of the camera.
- Dome Camera: A dome camera is a combination of camera, lens, and ceiling mount packaged in a discreet dome shape.
- PTZ Camera: A PTZ camera contains mechanical controls that allow the operator to remotely pan, tilt, and zoom the camera.
- Bullet Camera: A bullet camera is a combination of camera, lens, and housing packaged in a bullet-style body.
- IP Camera: An IP camera transmits a digital signal using Internet Protocol over a network
- Wireless IP Camera: Wireless IP security cameras offers ease of installation and eliminates the cost of network cabling when adding this camera to your video surveillance system.
- Day/Night Camera: A Day/night camera is a camera used indoor and outdoor for environments with low light conditions.
- Wide Dynamic Cameras: Wide Dynamic Cameras can balance light-levels on a pixel-by-pixel basis
- Smart/Doorbell Cameras: cameras typically affixed to a or inside of a residence.

Security Cameras supports the Department's mission and provides important operational value in the following ways:

X	Health	Protect safety of visitors and residents of San Francisco.
☐	Environment	
X	Criminal Justice	Review video footage after a crime has occurred or temporarily monitor, analyze, and resolve security risks during large-scale/significant events~~, or areas in city that pose security risks to visitors and residents~~.
☐	Housing	
X	Other	Effective public-safety interventions to curb crime and improve livability and wellbeing of communities.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Non-city entity Security Camera Systems do not require Department operational funding and reduce reliance on first-hand accounts by patrol officers or fixed posts, making deployments more effective and efficient.
X	Time Savings	Non-city entity Security Camera Systems may run 24/7, thus decreasing or eliminating building or patrol officer supervision. Reviewing Third

		Party data may also decrease demands on investigative units corroborating first-hand accounts of criminal activity.
X	Staff Safety	Non-city entity Security Camera Systems provide situational awareness and increase officer safety, particularly during live video reviews.
X	Service Levels	Non-city entity Security cameras will enhance effectiveness of incident response, criminal investigations, and result in improved level of service. Criminal activity captured through video can help verify the act of the crime and corroborate whether a suspect has been correctly identified and corroborate witness statements to assist with conviction rates.

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 Non-city entity, including PII, shall be classified according to the City's Data Classification Standard.

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

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 4
Date and Time	MP4 or other format	Level 4
Geolocation data	TXT, CSV, DOCX	Level 4

Notification: Departments shall rely on the non-city entity vendor to manage public notifications relating to 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.

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 members who have receive authorization from their officer and charge and have reviewed this policy, connected written directives, and acknowledged on SFPD Power DMS.

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 with Level 4 classification:

- Non-sworn members, at the direction of Officer in Charge. The Officer in Charge (OIC) is any member working in a supervisorial capacity over a unit, group, or team. The OIC is not rank specific.
- Q2-Q4, Police Officer
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain
- 0488-0490, Commander
- 0400-0402, Deputy Chief
- 0395, Assistant Chief
- 0390, Chief of Police

Live monitoring requests shall be limited to the following roles and job titles upon authorization of a Captain (Q80-Q82) rank:

- Q2-Q4, Police Officer
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain

The approving Captain shall use reliable and reasonable information relating to the likelihood of criminal activity for the basis of approving or denying live monitoring requests. Upon Board of Supervisors approval of this policy ordinance, the Department's Written Directives Unit will create and issue a standardized form for the ranks Q2 – Q62 to receive Captain rank approval. The form may be provided to the non-city entity to substantiate the SFPD live monitoring request. The non-city entity retains the right to refuse the request.

Live monitoring viewing rights include the following roles and job titles:

- Q2-Q4, Police Officer
- Q50-Q-52, Sergeant
- Q38, Inspector
- Q60-Q62, Lieutenant
- Q80-Q82, Captain
- 0488-0490, Commander
- 0400-0402, Deputy Chief
- 0395, Assistant Chief
- 0390, Chief of Police

B. Members of the public

Members of the public may 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 non-city entity (or shared by non-city entity) 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 non-city entity from unauthorized access and control, including misuse:

- Storage: Any storage of a non-city entity's camera footage must reside in a SFPD specified repository that meets the City's cyber security requirements as well as Department of Justice California Law Enforcement Telecommunications Systems (CLETS) and Criminal Justice Information Services (CJIS) requirements. Video Retrieval Officers may initially store footage provided by a business or individual on a USB or CD. Upon the execution of a city contract with a digital evidence management system vendor, members shall transfer the footage to this system that requires an agency domain and log in. The evidence management system will have a platform that is auditable and can track the source of upload and number of views. This platform will not be accessible to members of the public or anyone without an approved log-in. This platform will meet the requirements of the Office of Contract Administration ("OCA") who promulgates rules and regulations pursuant to Chapter 21 of the San Francisco Administrative Code. The SFPD Contracting Department shall

	comply with the requirements of Chapter 21 and cooperate to the fullest extent with OCA in the Acquisition of Commodities and Services. - Audits: SFPD members shall note in the chronological file ("chron") when surveillance footage was requested, approved, or denied by non-city entity, and in the case of live monitoring requests, Captain's approval, date/time of access, duration of access and outcome of access. Upon implementation of the internal records management system, SFPD members shall note this information in this system. This data will serve as the Department's audit log, which is electronically accessible for on-demand audits
Data Sharing:	The Non-city entity is the custodian of its Surveillance Technology data. The non-city entity may share such data with the Department or other entities solely at its discretion. Data is shared by non-city entity with the Department on the following schedule: X Upon Request X As needed Weekly Monthly Other: *A. Internal (City Entity) Data Sharing* Department shares the following data with the recipients: -District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence. -Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with California discovery laws. -The Department of Police Accountability per Section 4.136(j) of the Sn Francisco Charter -Other City agencies impacted by a criminal incident captured by the surveillance camera footage. Data sharing occurs at the following frequency: As needed *B. External (Non-City Entity) Data Sharing* Department shares the following data with the recipients: -Law enforcement partners, as part of a criminal or administrative investigation; Parties to civil litigation, or other third parties, in response to a valid Court Order; Media may receive redacted footage relating to Officer

Involved Shooting Townhall meetings or other public safety issues requiring the public's awareness or assistance.
To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Comply with all applicable laws, rules, and regulations, including but not limited to, to the extent applicable, the California Values Act (Government Code Section 7284 et seq.) which prohibits state and local law enforcement agencies from engaging certain acts related to immigration enforcement.

If determined by Department's general counsel or SFPD's legal division, surveillance camera footage can be disclosed in response to a public information request. Based on legal advice, the department will redact PII as it may be considered investigative/evidentiary material. The Department may use its discretion when releasing investigative/evidentiary material per SFPD DGO 3.16.

Data sharing occurs at the following frequency: As needed

Data Retention:

Department may store and retain PII data shared by the non-city entity only as long as necessary to accomplish a lawful and authorized purpose. Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files two years from the last date of entry with the following exceptions:

a) Information may be maintained if it is part of an ongoing investigation or prosecution.

b) All investigative files shall be maintained according to CA Penal Code, Evidence Code, department retention guidelines and according to state and federal law.

c) Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure.

It shall be the policy of the SFPD that once the requisite retention period for a record has passed, the record shall be destroyed unless there are circumstances that dictate that the record be retained.

The Department's data retention period and justification are as follows:

- Security Camera data shared with Department by Non-city entity will be stored only for the period necessary for investigation or litigation following an incident. If the data is associated with a criminal investigation, the data is retained for two years, or as required by State evidence retention laws.

- Justification: A shorter retention period safeguards PII from inappropriate or unauthorized use by minimizing the period and purposes for which it may be retained. For data affiliated with criminal investigation, 2 years allows adequate time for the Department and partner departments to access footage to determine whether it constitutes meaningful evidence. If so determined, the SFPD will retain data in a safe environment as required by relevant evidence laws to ensure access for legal discovery.

Data may 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 Disposal:	The Police Department does not have a contract or legal agreement with a non-city entity governing non-city entity data use, including but not limited to non-city entity party data use, sharing, signage, retention, and/or disposal. Upon completion of the data retention period, Department shall dispose of data in the following manner: - Delete from local storage - Delete from USB thumb drive or disk if not associated with investigative file
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. California Peace Officer Standards and Training (POST) including but not limited to - LD 15 - Laws of Arrest - LD 16 Search and Seizure - LD 17 Presentation of Evidence - LD 23 Crimes in Progress - LD 26 Critical Incidents - LD 30 Crime Scenes, Evidence, and Forensics - LD 42 Cultural Diversity/Discrimination - LD 43 Terrorism Awareness - PC 872 (b) Hearsay Testimony SF City & County Employee Portal - Cybersecurity Training

SFPD Training

- Critical Mindset Coordinated Response Training
- DGO 8.10 Guidelines for First Amendment Activities
- Video Retrieval Training (two-day)
- Crowd Control Training

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.

Allegations of 19B Violations: Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org. If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation. The Department will comply with allegation and misconduct processes as set forth by the city Charter.

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.

Sanctions for violations of this Policy include the following:
San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit or may refer the case to the Department of Police Accountability. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the Department of Police Accountability. Depending on the severity of the allegation of misconduct, the Chief or the Department of Police Accountability may elect to file charges with the Police Commission for any penalty greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

DEFINITIONS

Personally Identifiable Information (PII):	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.
Criminal Investigations:	A crime is an action or omission that constitutes as an offense that may be prosecuted by the government and is punishable by law.

	A criminal investigation is an official effort to uncover information about a crime. This is a process of discovering, collecting, preparing, identifying, and presenting evidence to determine whether a crime is occurring, has occurred and who was responsible.
Significant Events:	These are large or high-profile events in the city where SFPD Special Events Unit and Traffic Company manage street closures, barricades, and crowd management; Special Investigations Division (SID) manages dignitary escorts; or Homeland Security Unit (HSU) is assigned to thwart potential terrorist or criminal attacks. These units may require and request additional deployment efforts during these high-profile events based on activity detected during live monitoring which allows for situational awareness and the ability to coordinate resources based on information obtained.

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

Complaints of Officer Misconduct: Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA), 1 Van Ness Ave 8th Floor, San Francisco, CA 94103, (415) 241-7711, https://sf.gov/departments/department-police-accountability. DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD. DPA manages, acknowledges, and responds to complaints from members of the public.

Concerns and Inquiries: Department shall acknowledge and respond to concerns in a timely and manner. To do so, the Department has included a 19B Surveillance Technology Policy page on its public website : https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies. This page includes an email address for public inquiries: SFPDChief@sfgov.org. This email is assigned to several staff members in the Chief's Office who will respond to inquiries within 48 hours.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org