Surveillance Technology Policy

San Francisco Municipal Transportation Agency
Security Cameras

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 San Francisco Municipal and Transportation Agency (Department) aims to ensure the responsible use of department's Security Camera System, 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

This Surveillance Technology Policy ("Policy") defines the manner in which the Security Camera System (fixed or mobile) will be used to support Department's operations.

This Policy applies to all to Department personnel that use, plan to use, or plan to secure Security Camera Systems, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with Department are required to comply with this Policy.

POLICY STATEMENT

Department will limit its use of Security Camera Systems to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring.
2. Recording of video, images and review in the event of an incident.
3. Reviewing camera footage and/or images.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.
5. Enforcing parking and driving violations.

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

Further, processing of data from Department' Surveillance Technologies to identify the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or sex life or sexual orientation of an individual or group of individuals shall be prohibited. The processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: August 4, 2021

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras 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; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
☐	Jobs	
☐	Housing	
X	Other	Job Training and Safety – Review video footage from on-board cameras to train transit operators and improve on-board conditions and safety for customers.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Department's Security Camera Systems saves on building or patrol officers.
X	Time Savings	Department's Security Camera Systems run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct 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	Travel Time Savings -- Security cameras at key intersections help ensure clear and safe paths of travel for all surface modes. Security cameras in subway tunnels help ensure clear and safe paths of travel for sub-surface modes.

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 security cameras must be kept up-to-date and maintained.

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

The surveillance technology collects 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 intended surveillance technology operation at publicly accessible sites through signage in readily viewable public areas at those site. Department notifications shall identify the type and purpose of technology being used.

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
- ☐ Will persons be individually identified
- ☐ Data retention
- ☐ Department identification
- X Contact information

Access: Prior to accessing or using data from Department's Security Camera System, 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 Security and IT 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. - 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 Sharing:	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 will endeavor to ensure that other agencies or departments that may receive data collected by Department's 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. Each department that believes another agency or department receives or may receive data collected from its use of Security Cameras should consult with its assigned deputy city attorney regarding their response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: 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	Redact names, scrub faces, and 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 residents.
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.
X	Ensure shared data will be done 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 federal and State civil procedure laws and rules.

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 operating Department
- Police
- City Attorney
- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other local police departments

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 be aligned 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:

- In accordance with California Government Code section 34090.8(b), Department's Security Camera data will be stored for a minimum of one month or as long as the installed technology allows to be available to authorized staff for operational necessity and ready reference.

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

- Justification: 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 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 SFMTA Data Center

X Software as a Service Product

☐ 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) or specific Department training tailored to their specific role.

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.
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."

Appendix A: Department Specific Responses

1. **Products and Vendors the department uses:**

    a. The department maintains varies surveillance cameras throughout San Francisco. Although there are various legacy systems that are still in operation, the department has been working to standardize surveillance systems. The legacy systems use the same technology but may not be from the standard vendors.

    b. The departments typical security cameras are IP based cameras that are supplied by Hanwa or Axis. These cameras stream video footage across the network to the datacenter where video management solution (VMS) stores the footage. Genetec is the manufacturer of our VMS platform.

    c. Mobile video recorders from DTI (a third-party vendor) are used in buses and trains to record footage from inside and outside of the vehicle. This digital video recording (DVR) technology captures digital, color images and allow easier transmission, storage, and portability of those images.

    d. DriveCam is a G-Force triggered digital event recorder that saves triggered events and forwards them via the Internet. Each video is scanned for behavior-based actions and then analyzed by DriveCam safety experts and commented on accordingly. These analyzed events and data are then sent back to the client (SFMTA) for review and follow up in order to identify and address behavior-based actions that triggered the recording.

2. **General locations of cameras installed to help monitor the safety of patrons and staff.**

System	Description
SFGO	Cameras installed on signal poles
Facilities	Locations where employees work
Transit platforms and subway	Locations where the public wait to access our vehicles
PARCS (Parking Access and Revenue Control System)	Cameras in our parking garages
Transit Vehicles	Cameras installed in Buses, LRV's Cable Cars, etc.

3. Titles of Individuals authorized to access, or use collected information

SFMTA has staff that reviews video as part of their normal job responsibilities. They do this for varies operational reasons such as but not limited to; monitoring security events, reviewing operational efficiencies, customer service, and safety monitoring. This access is granted to select staff if their job role justifies access and that such access is restricted to specific area that is appropriate based on their needs.

Security Officers

Contract Security Officers, located in the Revenue Basement at One South Van Ness, monitor the Revenue Processing facility, and Customer Service Center at 11 South Van Ness on 24 hour/7 days a week (24/7) basis. Officers are also stationed and monitor Muni Metro East at 601 25th Street.

Remote sites are monitored after normal business hours and on weekends by Security Operations Center (SOC) Supervisors.

Parking Staff

It is the responsibility of the Parking Division (or their garage management contractor) to monitor their site(s). All requests for video shall be directed to or coordinated with the Video Surveillance Program Manager, following all SFMTA procedures and applicable laws in handling requests from law enforcement agencies and/or public records request. Internal request for video shall be directed to Parking Division Management who shall notify the Video Surveillance Program Manager.

Parking Staff Job Classification Details:

2 - 1824 Pr. Administrative Analyst
3 - 91xx Managers

Garage Operators

The Parking Division delegates the day to day operational activities to contracted companies to ensure our parking garages are well maintained. The local contractors will have at least view access to the local cameras to ensure they can monitor the facility in real time. The Parking staff may delegate additional work and access to the garage operators as they see fit.

Transit Division Staff

The Transit Division includes the following units: *Operations, Planning & Schedules*; *Transit Administration; Transit Services; Transit Management; and Bus and Rail Maintenance Units*. All requests for video data must follow the procedure(s) outlined in this document. While all of Transit can utilize and benefit from the various video cameras deployed by SFMTA, the following Units use or have need of use of SFMTA's Video Surveillance System on a regular or day-to-day basis:

a. Transit Services

Transit Services is a primary user of surveillance data and has authorized personnel who have specific need to view/review both live and recorded video data. Use of such data or recordings shall be done in a manner that protects the privacy of the public in accordance with this SFMTA policy.

Transit Services shall use video in response to a specific need and where a review of such data would contribute to the following:

- Review of a traffic operations or safety problem(s);
- Provision of a training review for future operator training;
- Research activities that will improve future technology or operations;
- Post-incident review of a particularly complex incident and/or emergency for the purposes of improving operations procedures and response;
- Demonstrating, testing equipment or system functions;
- Collection of data for transportation planning management purposes

Transit Staff Job Classifications Details:

5 - 91xx– Managers
1 - 9160 –Transit Operations Specialist

b. Transportation Management Center (TMC) Staff

Transportation Management Center (TMC) is responsible for management and administration of the operations workforce for all transit modes: bus, rail and cable car, staff scheduling, dispatching, workforce planning and day-to-day contract administration. The TMC monitors roadway

conditions, provides support to SFMTA drivers/operators and field personnel responding to rail or roadway incidents, which enhances effectiveness of transit operations and enables the active management of traffic flow.

Except as provided for in this document, SFMTA surveillance video shall not be disseminated by TMC staff. The TMC shall receive surveillance video in a real-time or a limited-time-delay data feed. Furthermore, the TMC shall use and/or review the data for transit operations, maintaining and improving safety.

TMC Staff Job Classifications Details:

2 - 91xx – Managers
1 - 9160 – Transit Operations Specialist
2 - 915x – Transportation Controllers
1 - 9139 – Transit Supervisor

4. Public Record Requests for Video

The Video Surveillance Program Manager is responsible for ensuring that Video Surveillance Program staff respond to Public Records Requests for video in accordance with SFMTA's Public Records Policy and Procedure guidance document.

Video recordings are public records and disclosure is governed by the California Public Records Act (Government Code Section 6252) and the City's Sunshine Ordinance, Chapter 67 of the San Francisco Administrative Code. Sec **Error! Reference source not found.**.

In compliance with state and local law, video recordings are generally released in response to a public records request unless there is an applicable exemption, such as a pending law enforcement investigation, provided for under state or local law.