Surveillance Technology Policy

Driver-Safety Video Analytics
Municipal Transportation Agency

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 Driver-Safety Video Analytics 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 connect San Francisco through a safe, equitable, and sustainable transportation system.

This Surveillance Technology Policy ("Policy") defines the manner in which Driver-Safety Video Analytics will be used to support this mission, by describing its intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Driver-Safety Video Analytics, 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 authorized use of Driver-Safety Video Analytics for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– *To identify collision dynamics, causation, and other factors.*
– *To investigate passenger fall events and exploring potential safety improvements.*
– *To identify infrastructure (damaged or vandalized bus stop shelters, downed or hazardous trees, etc.) and signage issues (signs obscured by graffiti or by a low hanging or overgrown tree or shrub, etc.) as they relate to MTA transit service and safety.*
– *To review customer complaints and look for potential ways to improve safety and service.*
– *To identify driver training issues, misconduct, or negligence.*
– *To commend drivers who demonstrate outstanding defensive driving skills.*

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

Surveillance Oversight Review Dates
PSAB Review: 01/27/2023 ("Recommended: 02/24/2023")
COIT Review: TBD (list all dates at COIT, and write "Recommended: MM/DD/202X" for rec date)
Board of Supervisors Approval: TBD

Departments may use information collected from surveillance 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. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Reason for Technology Use

Use of Driver-Safety Video Analytics supports the Department's mission and provides important operational value in the following ways:

By enhancing our efforts to identify local transit and regional transportation safety issues, comply with training standards, rules, and vehicle code laws, and determine the likely causations for vehicle collisions and passenger falls.

Description of Technology

This technology uses video and audio event recorders together with proprietary, vendor-owned algorithms to record and identify certain behavior-based safety events, such as operator looking at cell phone while driving.
The event recorders are triggered by excess g-forces (e.g., collision impacts, abrupt braking, excessive turning, etc.) and capture eight seconds of video/audio prior to the trigger, and four seconds after the trigger, for a total of 12 seconds of video and audio. Once recorded, the proprietary algorithm categorizes the event into one of several predefined safety events, which are then reviewed by the vendor for accuracy. If accurate, the vendor notifies and sends the recording to the department for further review.

Resident Benefits

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

	Benefit	Description
▪	Education	
▪	Community Development	
▪	Health	
▪	Environment	
▪	Criminal Justice	
▪	Jobs	
▪	Housing	

X	Other: Public Safety	The technology allows the department to identify and target for training opportunities specific driver behaviors that trigger safety events so it can minimize these behaviors in the future and improve public safety.

Department Benefits

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

	Benefit	Description
▪	Financial Savings	
▪	Time Savings	
X	Staff Safety	The G-Force video capture and AI-based algorithms enhance the mission of the Safety Division to improve safety procedures, identify training needs and identifies exemplary employees without the need for hundreds of additional personnel that it would require to gain the same insights that the technology provides.
X	Data Quality	It enhances the safety and training procedures\, identifies engineering needs\, and identifies exemplary employees without the need for hundreds of additional personnel that it would require to gain the same insights that the technology provides.
X	Other: Operator training	The technology allows the department to identify and target for training opportunities specific driver behaviors that trigger safety events so it can minimize these behaviors in the future and improve operator performance.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department's use of Driver-Safety Video Analytics 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)	*Format(s)*	*Classification*
Video and audio images	MP4	Level 3
Reports	HTML, downloaded as PDFs	Level 3

Notification:

Department provides no public signage or notification in connection with Driver-Safety Video Analytics because Department does not use Driver-Safety Video Analytics to monitor or record passengers or other members of the public; The Department uses Video Safety Analytics to monitor incidents triggered by specific driver behaviors (speeding, rolling stops, etc.) or identified by specific AI algoritms (Talking on cell phone, eating while driving, drowsy/sleeping, etc.)".

Access: All parties requesting access to surveillance technology or data from [surveillance technology] must adhere to the following rules and processes:

- Prior to any person gaining access and use of the Driver-Safety Video Analytics and data, they must:
  - Have an SFMTA manager or supervisor authorize that person for access to the Driver-Safety Video Analytics web portal (Drivecam); New users cannot request access directly from the Drivecam administrator. That same authorizing manager or supervisor must notify the SFMTA Drivecam administrator and request that a user name and password for the new person be generated, and to what degree that access should be allowed.;(Access can be Read Only, Coach, or Safety Manager).
  - The Department's Driver-Safety Video Analytics administrator then enters that person as a user and sends instructions to that new user on how to login to the Drivecam web site. If the new user has never before been an authorized user, the department administrator cautions the new user in writing that the Driver-Safety Video Analytics videos and/or Driver-Safety Video Analytics reports are considered confidential personnel records and shall not be viewed, discussed, or forwarded to any

unauthorized person within the department, and with no other person outside of the department without; specific written permission;

- All department emails that contain an attached Driver-Safety Video Analytics or data report shall have in the Subject line of the email the following phrase: CONFIDENTIAL PERSONNEL MATTER. Investigators and attorneys employed by the San Francisco City Attorney may be granted access upon request made directly to the department's Chief Safety Officer or other department upper manager. Members of Law Enforcement agencies shall not be given access to the department's Driver-Safety Video Analytics web pages. However, upon written request from an investigating officer of a law enforcement agency describing the specific investigative need for any Driver-Safety Video Analytics video or data; report, videos may be provided upon the authorization of the department's Chief Safety Officer.
- All Driver-Safety Video Analytics videos and data reports provided to an authorized law enforcement investigator shall be cautioned that Driver-Safety Video Analytics reports are considered confidential personnel records and shall not be viewed, discussed, or forwarded to any unauthorized person.

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:

- 9183 Deputy Director, Chief Safety Officer (CSO)
- 1406 Senior Clerk (4staff)
- 1820 Junior Administrative Analyst (4 staff)
- 1823 Senior Administrative Analyst
- 1840 Junior Management Assistant
- 5177 Safety Officer
- 6130 Safety Analyst
- 9172 Manager IIMTA (2 staff)
- 9520 Trans Safety Specialist 10 (2 staff)

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.

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 other applicable law.

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 require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

Department training will include:

The training is basic navigation of the Driver-Safety Video Analytics site pages that houses our account and the events generated by the technology. There are other technical types of training for the maintenance crews.

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.

The technology provider for the rubber tires, Lytx, receives recorded transmitted video from the Video Event Recorder (VER) to Lytx's backend over an encrypted connection, and upon arrival to their Lytx cloud, video clips are encrypted at rest. Encryption at rest is a way to prevent the attacker from accessing data when it is saved in the disk/hard-drive. Moreover, Lytx has been asked not to view the live video feed from the DriveCam cameras, if system allows live viewing. The on-board recorder stores audio/video data on the SD card which is encrypted with 128-bit AES at rest. Lytx's primary production servers are located in two geographically separated

N-tier (redundancy). Each datacenter is SSAE-18 (Statement on Standards for Attestation Engagements 18 – based on industry standards) certified, and provide 24/7 physical security monitoring, including biometric access controls. These datacenters are SOC2 Type 2 (Organization Control) attestation related to security, availability, and confidentiality. A SOC 2 Type 2 report is an internal controls report capturing how a company safeguards customer data and how well those controls are operating. Companies that use cloud service providers use SOC 2 reports to assess and address the risks associated with third party technology services.

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

The Department Driver-Safety Video Analytics administrator shall:

- Conduct or have conducted a review of the list of authorized Driver-Safety Video Analytics users periodically throughout any given calendar year to determine the need to disable access of users who:
  - Have not logged into the Department Driver-Safety Video Analytics web pages within the past 365 days (except for active middle managers and supervisors).
  - Have retired or otherwise left the employment at the Department.
  - Have been reassigned to a position within the Department that does not have a demonstrative need for Driver-Safety Video Analytics access.
  - Have deceased.
  - Have had their authorization revoked by a Department manager or supervisor.

Misuse of access to the Department's Driver-Safety Video Analytics site shall be referred to that person's immediate supervisor or manager for follow up.

Data Storage: 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.)

- Department of Technology Data Center
- Software as a Service Product
- Cloud Storage Provider

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 the surveillance technology will act in conformity with 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
Video Recording	Access may be provided after SFPD written request approved by the Chief

	Safety Officer, City Attorney's Office (CAO).

Frequency - Data sharing occurs at the following frequency:
Frequency varies. On average 2 or 3 times per year and upon specific, written request for investigative purposes by the Police Department; 2 to 4 times per month by the City Attorney.

B. External Data Sharing:

Yes. Department shares data with provider (Lytx) for analysis.

Data Type	Data Recipient
Video Recording	Lytx

Reporting Frequency - An example of such frequency is the following: For the 6-month period of August 2022 thru January 2023, the department's rubber-tire fleet of 845 Drivecam-Equipped busses (includes trolley-coaches) generated a combined total of 8,321 Drivecam events. Of that number:

- 883 (10.6%) were assessed by Lytx and returned to the department for further action.
- 47 (0.57%) were confirmed traffic collisions but were not assessed by Lytx (as per our contract). Lynx provides, to the department, the factual dynamic data associated with each collision, such as location, date/time, speed of the bus, type of trigger, and g-forces of turns.
- 21 (0.25%) were confirmed passenger falls but were not assessed by Lytx. As with collisions, dynamic data was provided.
- 991 (12%) were identified as "Near-Collision Unavoidable" by Lytx, but not assessed. All dynamic data was provided to the department.

Of the total 8,321 Drivecam events, only 1,942 (24%) events required a follow up action by the department (i.e., training, discipline, safety analysis, infrastructure analysis, driver commendation).

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
[Video and PDF Reports (by Department) is retained 365 days by vendor and then on day 366 it is deleted. If the video warrants further investigation based on use cases stated above, then the Department may retain the video longer on its servers. All video uploaded to the Lytx data center is retained and available for 90 days and then stored on backup media for an additional 275 days	Investigations and additional training needs appropriate amount of time to be scheduled and video is key to training efforts. Technology is only used when g- force exceeds a predefined threshold. Video and PDF Reports (by Department) is often needed by the City Attorney for civil litigation; therefore, Department needs to retain video for a longer period of time.

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):

- Investigations and additional training needs appropriate amount of time to be scheduled and video is key to training efforts. Technology is only used when g-force exceeds a predefined threshold. Video is often needed by the City Attorney for civil litigation, therefore the Department needs to retain video for a longer period of time

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: DriveCam -Video Analytics data is disposed of by the system on the 366th day.
- Processes and Applications: Videos are automatically deleted from the data center on 91st day and deleted from the backup media on the 276th day on first in first out basis.

COMPLIANCE

Department 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

Oversight Personnel

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

- Chief Safety Officer – 9183
- Deputy Director Manager, Budget; Administration – 9172
- Manager II Drivecam Administrator – 9172

Sanctions for Violations

Sanctions for violations of this Policy include the following:

Violations of this Policy may result in disciplinary action commensurate with the severity of violation. Sanctions may include written warning, suspension, and termination of employment.

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, is data collected, retained, or processed by the department and shared with law enforcement.

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.
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

Members of the public may register complaints or concerns about the deployment of the technology through 311.org.

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

Department responds to all 311 complaints.

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.