File No. 220843 **Committee Item No.** 4
Board Item No. 32

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee **Date** Oct. 3, 2022

Board of Supervisors Meeting **Date** October 18, 2022

Cmte Board

☐	☐	**Motion**
☐	☐	**Resolution**
☒	☐	**Ordinance**
☒	☐	**Legislative Digest**
☐	☐	**Budget and Legislative Analyst Report**
☐	☐	**Youth Commission Report**
☐	☐	**Introduction Form**
☒	☐	**Department/Agency Cover Letter and/or Report**
☐	☐	**Memorandum of Understanding (MOU)**
☐	☐	**Grant Information Form**
☐	☐	**Grant Budget**
☐	☐	**Subcontract Budget**
☐	☐	**Contract/Agreement**
☐	☐	**Form 126 - Ethics Commission**
☐	☐	**Award Letter**
☐	☐	**Application**
☐	☐	**Form 700**
☐	☐	**Information/Vacancies (Boards/Commissions)**
☐	☐	**Public Correspondence**

OTHER **(Use back side if additional space is needed)**

☒	☐	Various Departmental Surveillance Tech Policies and Impact Reports.
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	

Completed by: Victor Young **Date** Sept 29, 2022
Completed by: _____ **Date** _____

AMENDED IN COMMITTEE
10/3/2022

FILE NO. 220843 ORDINANCE NO.

[Administrative Code - Approval of Surveillance Technology Policies for Multiple City Departments]

Ordinance approving Surveillance Technology Policies governing the use of 1) Automatic License Plate Readers by the Municipal Transportation Agency, 2) Biometric Processing Software or System by the Juvenile Probation Department, 3) Body-Worn Cameras by the Fire Department ~~and Recreation and Park Department~~**, 4) People-Counting Camera by the Library,** ~~5) Security Cameras by the Department of Elections,~~ 6~~5~~**) Third-Party Security Cameras by the** ~~Airport,~~ **Municipal Transportation Agency**~~, Police Department,~~ **and War Memorial,** ~~7~~6**) Location Management Systems by the Juvenile Probation Department** ~~and the Recreation and Park Department,~~ 8~~7~~**) Computer Management System by the Library, and** ~~9~~8**) Social Media Monitoring Software by the Library; and making required findings in support of said approvals.**

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in ~~*strikethrough italics Times New Roman font*~~.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. Background.

(a) Terms used in this ordinance shall have the meaning set forth in Administrative Code Chapter 19B ("Chapter 19B").

(b) Chapter 19B regulates City Departments' acquisition and use of Surveillance Technology. Under Section 19B.5, City Departments that possessed or were using Surveillance Technology before Chapter 19B took effect in July 2019, must obtain Board of

Supervisors approval by ordinance of a Surveillance Policy for each type of existing Surveillance Technology. Under Section 19B.2, a Department must obtain Board of Supervisors approval by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Surveillance Technology Policy ordinance approved by the Board in accordance with Chapter 19B; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering into an oral or written agreement under which a non-City entity or individual regularly provides the Department with data or information acquired through the entity's use of Surveillance Technology.

(c) Beginning in August 2019, Departments submitted to the Committee on Information Technology ("COIT") inventories of their existing Surveillance Technology and submitted Surveillance Impact Reports for each type of Surveillance Technology on their inventory.

(d) After receiving the inventories and Surveillance Impact Reports, COIT and its Privacy and Surveillance Advisory Board ("PSAB") subcommittee, conducted multiple public hearings, at which COIT and PSAB considered both the inventories and Surveillance Impact Reports for existing Surveillance Technology. Following those hearings, COIT developed Surveillance Technology Policies for multiple Departments covering ~~eight~~seven categories of Surveillance Technology:

(1) Automatic License Plate Readers (ALPR)

(2) Biometric Processing Software or System

(3) Body-Worn Cameras

(4) People-Counting Cameras

~~(5) Security Cameras~~

(~~6~~5) Third-Party Security Cameras

(~~7~~6) Location Management System

(~~8~~7) Computer Management System

(e) Additionally, the Library submitted a Surveillance Impact Report for Social Media Monitoring Software~~ and the Recreation and Park Department submitted a Surveillance Impact Report for a Location Management System~~. Based on the Surveillance Impact Report~~s~~, COIT developed a Surveillance Technology Policy for Social Media Monitoring Platforms used by the Library~~, and a Surveillance Technology Policy for a Location Management System used by the Recreation and Park Department~~.

(f) The Surveillance Technology Policies that COIT developed for each Department are detailed in Sections 2 through ~~10~~9 of this ordinance. The Surveillance Technology Policies are available in Board File No. 220843, and are incorporated herein by reference. COIT recommends that the Board of Supervisors approve each Surveillance Technology Policy.

(g) This ordinance sets forth the Board's findings in support of each Surveillance Technology Policy and its approval of each policy.

Section 2. Automatic License Plate Readers ("ALPR"): Municipal Transportation Agency ("MTA").

(a) Current Status. MTA currently possesses and uses ALPR.

(b) Purpose. MTA uses an ALPR ("MTA ALPR") to: (1) enforce parking restrictions and laws; (2) Transit Only Lane Enforcement; (3) link individual vehicles to their times of entry/exit into City-owned parking garages and lots to accurately calculate parking fees; (4) identify vehicles that are the subject of an active investigation by the Police Department; and (5) analyze and report on parking and curb usage.

(c) Surveillance Impact Report. MTA submitted a Surveillance Impact Report for MTA ALPR to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(d) Public Hearings. Between September 9, 2021 and October 21, 2021, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the MTA ALPR ("MTA ALPR Policy"). A copy of the MTA ALPR Policy is in Board File No.220843, and is incorporated herein by reference.

(e) COIT Recommendation. On October 21, 2021, COIT voted to recommend the MTA ALPR Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that the benefits that the MTA ALPR Policy authorizes outweigh the costs and risks; that the MTA ALPR Policy will safeguard civil liberties and civil rights; and that the uses and deployments of MTA ALPR, as set forth in the MTA ALPR Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(g) Approval of Policy. The Board of Supervisors hereby approves the MTA ALPR Policy under which MTA may continue to possess and use the MTA ALPR.

Section 3. Biometric Processing Software or System (Continuous Alcohol Monitoring "CAM" technology): Juvenile Probation.

(a) Current Status. Juvenile Probation currently possesses and uses CAM technology.

(b) Purpose. Juvenile Probation uses CAM technology known as SCRAM CAM to monitor alcohol consumption among youth on court-ordered probation as a condition of their probation.

(c) Surveillance Impact Report. Juvenile Probation submitted a Surveillance Impact Report for SCRAM CAM to COIT. A copy of the Juvenile Probation Surveillance Impact Report for SCRAM CAM is in Board File No. 220843, and is incorporated herein by reference.

(d) Public Hearings. On January 14, 2022 and February 17, 2022, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Juvenile Probation's use of SCRAM CAM ("Juvenile Probation SCRAM CAM Policy"). A copy of the Juvenile Probation SCRAM CAM Policy is in Board File No. 220843, and is incorporated herein by reference.

(e) COIT Recommendation. On February 17, 2022, COIT voted to recommend the Juvenile Probation SCRAM CAM Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that: the benefits authorized by the Juvenile Probation SCRAM CAM Policy outweigh its costs and risks; that the Juvenile Probation SCRAM CAM Policy will safeguard civil liberties and civil rights, and that the uses and deployments of SCRAM CAM, as set forth in the Juvenile Probation SCRAM CAM Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(g) Approval of Policy. The Board of Supervisors hereby approves the Juvenile Probation SCRAM CAM Policy under which Juvenile Probation may continue to possess and use SCRAM CAM.

Section 4. Body-Worn Cameras: Fire Department ~~and Recreation and Park Department~~.

(a) Current Status. The following Department~~s~~ currently possesses and uses Body-Worn Cameras: the Fire Department~~; and the Recreation and Park Department~~.

(b) Fire Department.

(1) Purpose. The Fire Department's Public Information Officer (PIO) currently uses a Body-Worn Camera when on-scene at large incidents to capture video of surroundings and the totality of the incident.

(2) Surveillance Impact Report. The Fire Department submitted to COIT a Surveillance Impact Report for Fire Department Body-Worn Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(3) Public Hearings. On September 10, 2021, and October 21, 2021, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Fire Department Body-Worn Cameras ("Fire Department Body-Worn Cameras Policy"). A copy of the Fire Department Body-Worn Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.

(4) COIT Recommendation. On October 21, 2021, COIT voted to recommend the Fire Department Body-Worn Cameras Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits that the Fire Department Body-Worn Cameras Policy authorizes outweigh the costs and risks; that the Fire Department Body-Worn Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Body-Worn Cameras, as set forth in the Fire Department Body-Worn Cameras Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the Fire Department Body-Worn Cameras Policy under which the Fire Department may continue to possess and use the Body-Worn Cameras.

~~(c) Recreation and Park Department.~~

~~(1) Purpose. The Recreation and Park Department uses Body-Worn Cameras to record video and audio footage in the event of an incident, including actual or potential criminal conduct; in situations where a Park Ranger reasonably believes recordings of evidentiary value may be requested; and calls for service involving a crime where the recording may aid in the apprehension/prosecution of a suspect. The Recreation and Park Department also provides Body-Worn Camera recordings to law enforcement or other authorized persons upon request.~~

~~(2) Surveillance Impact Report. The Recreation and Park Department submitted a Surveillance Impact Report for Body-Worn Cameras to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(3) Public Hearings. On September 24, 2021 and October 21, 2021, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Recreation and Park Department Body-Worn Cameras ("Recreation and Parks Department Body-Worn Cameras Policy"). A copy of the Recreation and Parks Department's Body-Worn Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(4) COIT Recommendation. On October 21, 2021, COIT voted to recommend the Recreation and Parks Department Body-Worn Cameras Policy to the Board of Supervisors for approval.~~

~~(5) Findings. The Board of Supervisors hereby finds that the benefits that the Recreation and Parks Department's Body-Worn Cameras Policy authorizes outweighs its costs and risks; that the Recreation and Parks Department Body-Worn Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of the Body-Worn Cameras, as set forth in the Recreation and Parks Department Body-Worn Cameras Policy,~~

~~will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.~~

~~(6) Approval of Policy. The Board of Supervisors hereby approves the Recreation and Parks Department Body-Worn Cameras Policy under which the Recreation and Park Department may continue to possess and use the Body-Worn Cameras.~~

Section 5. People-Counting Camera: Library.

(a) Current Status. The Library currently possesses and uses People-Counting Cameras.

(b) Purpose. Library uses People-Counting Cameras to: (A) tally the entry and exit of Library visitors at all 28 public facilities; and (B) track usage of meeting rooms, elevators, and restrooms for purposes of resource allocation.

(c) Surveillance Impact Report. The Library submitted a Surveillance Impact Report for Library People-Counting Cameras to COIT. A copy of the Library Surveillance Impact Report for Library People-Counting Cameras is in Board File No. 220843, and is incorporated herein by reference.

(d) Public Hearings. On January 28, 2022, March 11, 2022, and April 21, 2022, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the Library People-Counting Cameras. A copy of the Surveillance Technology Policy for the Library's use of the Library People-Counting Cameras ("Library People-Counting Cameras Policy") is in Board File No. 220843, and is incorporated herein by reference.

(e) COIT Recommendation. On April 21, 2022, COIT voted to recommend the Library People-Counting Cameras Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that: the benefits that the Library People-Counting Cameras Policy authorizes outweigh its costs and risks; that the Library People-Counting Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Library People-Counting Cameras, as set forth in the Library People-Counting Cameras Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(g) Approval of Policy. The Board of Supervisors hereby approves the Library People-Counting Cameras Policy under which the Library may continue to possess and use the Library People-Counting Cameras.

~~Section 6. Security Cameras: Department of Elections.~~

~~(a) Current Status. The Department of Elections currently possesses and uses Security Cameras.~~

~~(b) Purpose. The Department of Elections uses the Security Cameras to: (A) conduct live monitoring of voting center lines; (B) conduct live monitoring of Department staff during elections operations; (C) record video and images of Department staff during elections operations; (D) review camera footage of Department staff in the event of an incident; and (E) share camera footage of Department staff with the public to promote transparency into elections operations.~~

~~(c) Surveillance Impact Report. The Department of Elections submitted a Surveillance Impact Report for the Security Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(d) Public Hearings. On January 22, 2021, October 21, 2021, and November 18, 2021, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the Security~~

~~Cameras. A copy of the Department of Elections Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(e) COIT Recommendation. On November 18, 2021, COIT voted to recommend the Department of Elections Cameras Policy to the Board of Supervisors for approval.~~

~~(f) Findings. The Board of Supervisors hereby finds that: the benefits authorized by the Department of Elections Cameras Policy outweigh the costs and risks; that the Department of Elections Cameras Policy will safeguard civil liberties and civil rights, and that the uses and deployments of Cameras, as set forth in the Department of Elections Cameras Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.~~

~~(g) Approval of Policy. The Board of Supervisors hereby approves the Department of Elections Cameras Policy under which the Department of Elections may continue to possess and use the Security Cameras.~~

Section ~~7~~6. Third-Party Security Cameras: ~~San Francisco International Airport ("SFO"),~~ MTA~~,~~ and War Memorial and Performing Arts Center ("War Memorial").

(a) Current Status. The following Departments currently possess and use data from Third-Party Security Cameras: ~~SFO,~~ MTA~~,~~ and War Memorial.

~~(b) SFO.~~

~~(1) Purpose. SFO uses data from security cameras owned and operated by SFO tenants, including airlines, concessionaries, food and beverage operators, and rental car agencies ("Tenant Security Cameras"), to (A) review camera footage in the event of an incident; and (B) approve Airport tenants' disclosure of digital recordings and other data from its security camera.~~

~~(2) Surveillance Impact Report. SFO submitted a Surveillance Impact Report for Tenant Security Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(3) Public Hearings. Between January 14, 2022 and February 17, 2022, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for SFO Tenant Security Cameras ("SFO Tenant Security Cameras Policy"). A copy of the SFO Tenant Security Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(4) COIT Recommendation. On February 17, 2022, COIT voted to recommend the SFO Tenant Security Cameras Policy to the Board of Supervisors for approval.~~

~~(5) Findings. The Board of Supervisors hereby finds that the benefits authorized by the SFO Tenant Security Cameras Policy outweigh the costs and risks; that the SFO Tenant Security Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Tenant Security Cameras, as set forth in the SFO Tenant Security Cameras Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.~~

~~(6) Approval of Policy. The Board of Supervisors hereby approves the SFO Tenant Security Cameras Policy under which SFO may continue to possess and use the Tenant Security Cameras.~~

(~~c~~b) MTA.

(1) Purpose. MTA uses Third-Party Security Cameras owned and operated by taxi drivers that are located inside taxi cabs ("Taxi Dashboard Cameras") to: (A) review recordings of on-board incidents based upon complaints received from the public, and use at appeals hearings in response to a fine, suspension, or response to fine revocation; (B) review

video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the Transportation Code; (C) review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides; (D) review video to investigate criminal acts involving taxi drivers or riders; and (E) review video data to investigate accidents involving a taxi cab.

(2) Surveillance Impact Report. MTA submitted a Surveillance Impact Report for MTA Taxi Dashboard Cameras to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(3) Public Hearings. On March 11, 2022, and April 21, 2022, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the MTA Taxi Dashboard Cameras ("MTA Taxi Dashboard Camera Policy"). A copy of the MTA Taxi Dashboard Camera Policy is in Board File No. 220843, and is incorporated herein by reference.

(4) COIT Recommendation. On April 21, 2022, COIT voted to recommend the MTA Taxi Dashboard Camera Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits authorized by the MTA Taxi Dashboard Camera Policy outweigh the costs and risks; that the MTA Taxi Dashboard Camera Policy will safeguard civil liberties and civil rights, and that the uses and deployments of the MTA Taxi Dashboard Cameras, as set forth in the MTA Taxi Dashboard Camera Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the MTA Taxi Dashboard Camera Policy under which MTA may continue to possess and use the MTA Taxi Dashboard Cameras.

(~~d~~c) War Memorial.

(1) Purpose. War Memorial uses data from security cameras owned and operated by the San Francisco Symphony located at War Memorial venues ("Tenant Security Cameras") to: (A) live monitor Davies Symphony Hall internal and public areas; and (B) review camera footage in the event of an incident.

(2) Surveillance Impact Report. War Memorial submitted a Surveillance Impact Report for Tenant Security Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(3) Public Hearings. Between August 27, 2021, and April 21, 2022, COIT and PSAB conducted a total of four public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the Tenant Security Cameras ("War Memorial Tenant Security Cameras Policy"). A copy of the War Memorial Tenant Security Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.

(4) COIT Recommendation. On April 21, 2022, COIT voted to recommend the War Memorial Tenant Security Cameras Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that benefits authorized by the War Memorial Tenant Security Cameras Policy outweigh the costs and risks; that the War Memorial Tenant Security Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Tenant Security Cameras, as set forth in the War Memorial Tenant Security Cameras Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the War Memorial Tenant Security Cameras Policy under which War Memorial may continue to possess and use the Tenant Security Cameras.

Section ~~8~~7. Location Management System: Juvenile Probation~~ and Recreation and Park Department~~.

(a) Current Status. Juvenile Probation currently possesses and uses a Location Management System. ~~The Recreation and Park Department seeks to acquire and use a Location Management System.~~

(b) Juvenile Probation

(1) Purpose. Juvenile Probation uses a Location Management System known as SCRAM Global Positioning System ("SCRAM GPS") to enforce court-ordered supervision of youth placed on electronic monitoring as a condition of their probation or as an alternative to detention.

(2) Surveillance Impact Report. Juvenile Probation submitted a Surveillance Impact Report for SCRAM GPS. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(3) Public Hearings. On October 22, 2021 and November 18, 2021, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for SCRAM GPS ("Juvenile Probation SCRAM GPS Policy"). A copy of the Juvenile Probation SCRAM GPS Policy is in Board File No. 220843, and is incorporated herein by reference.

(4) COIT Recommendation. On November 18, 2021, COIT voted to recommend the Juvenile Probation SCRAM GPS Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits authorized in the Juvenile Probation SCRAM GPS Policy outweigh the costs and risks; that the SCRAM GPS will safeguard civil liberties and civil rights; and that the uses and deployments of SCRAM GPS, as set forth in the Juvenile Probation SCRAM GPS Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the Juvenile Probation SCRAM GPS Policy under which Juvenile Probation may continue to possess and use SCRAM GPS.

~~(c) Recreation and Park Department~~

~~(1) Purpose. The Recreation and Park Department would like to use a Location Management System to manage reservations for tennis facilities and determine if reservation holders are present at the tennis facility at the time of their reservation.~~

~~(2) Surveillance Impact Report. The Recreation and Park Department submitted a Surveillance Impact Report for a Location Management System to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(3) Public Hearings. On March 11, 2022, May 27, 2022, and June 16, 2022, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Location Management System ("Tennis Reservations Application Policy"). A copy of the Recreation and Park Department Tennis Reservations Application Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(4) COIT Recommendation. On June 16, 2021, COIT voted to recommend the Recreation and Park Department Tennis Reservations Application Policy to the Board of Supervisors for approval.~~

~~(5) Findings. The Board of Supervisors hereby finds that the benefits authorized by the Recreation and Park Department Tennis Reservations Application Policy outweigh the costs and risks; that the Location Management System will safeguard civil liberties and civil rights; and that the uses and deployments of the Location Management System, as set forth in the Recreation and Park Department Tennis Reservations Application Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.~~

~~(6) Approval of Policy. The Board of Supervisors hereby approves the Recreation and Park Department Tennis Reservations Application Policy under which the Recreation and Park Department may acquire and use the Location Management System.~~

Section ~~9~~8. Computer Management System: Library.

(a) Current Status. The Library currently possesses and uses a Computer Management System.

(b) Purpose. The Library uses a Computer Management System to provide time-delimited public access to library computers and allow the public to print, copy, scan, and fax documents, as well as to track usage of computers and print resources throughout Library facilities for purposes of resource allocation and management.

(c) Surveillance Impact Report. The Library submitted a Surveillance Impact Report for their Computer Management System to COIT. A copy of the Library Surveillance Impact Report for their Computer Management System is in Board File No. 220843, and is incorporated herein by reference.

(d) Public Hearings. On May 27, 2022, and June 16, 2022, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the Library Computer Management System. A copy of the Surveillance Technology Policy for the Library's use of the Library Computer Management System ("Library Computer Management System Policy") is in Board File No. 220843, and is incorporated herein by reference.

(e) COIT Recommendation. On June 16, 2022, COIT voted to recommend the Library Computer Management System Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that the benefits that the Library Computer Management System Policy authorizes outweigh its costs and risks; that the Library Computer Management System Policy will safeguard civil liberties and civil rights; and that the uses and deployments of the Library Computer Management System, as set forth in the Library Computer Management System Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(g) Approval of Policy. The Board of Supervisors hereby approves the Library Computer Management System Policy under which the Library may continue to possess and use the Library Computer Management System.

Section ~~10~~9. Social Media Monitoring Software: Library.

(a) Current Status. The Library seeks to acquire and use Social Media Monitoring Software.

(b) Purpose. The Library would like to use Social Media Monitoring Software to plan, execute, and analyze trends in communication campaigns across social media platforms.

(c) Surveillance Impact Report. The Library submitted a Surveillance Impact Report for Social Media Monitoring Software to COIT. A copy of the Library Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(d) Public Hearings. On August 27, 2021 and October 21, 2021, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Social Media Monitoring Software ("Library Social Media Monitoring Software Policy"). A copy of the Library Social Media Monitoring Software Policy is in Board File No. 220843, and is incorporated herein by reference.

(e) COIT Recommendation. On October 21, 2021, COIT voted to recommend the Library Social Media Monitoring Software Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that the benefits authorized by the Library Social Media Monitoring Software Policy outweigh the costs and risks; that the Social Media Monitoring Software will safeguard civil liberties and civil rights; and that the uses and deployments of Social Media Monitoring Software, as set forth in the Library Social Media Monitoring Software Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(g) Approval of Policy. The Board of Supervisors hereby approves the Library Social Media Monitoring Software Policy under which the Library may acquire and use the Social Media Monitoring Software.

Section ~~11~~10. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the

ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/ Zachary Porianda
ZACHARY PORIANDA
Deputy City Attorney

n:\govern\as2022\1900636\01632430.docx

FILE NO. 220843

LEGISLATIVE DIGEST
(Revised 10/3/2022)

[Administrative Code - Approval of Surveillance Technology Policies for Multiple City Departments]

Ordinance approving Surveillance Technology Policies governing the use of 1) Automatic License Plate Readers by the Municipal Transportation Agency, 2) Biometric Processing Software or System by the Juvenile Probation Department, 3) Body-Worn Cameras by the Fire Department, 4) People-Counting Camera by the Library, 5) Third-Party Security Cameras by the Municipal Transportation Agency and War Memorial, 6) Location Management Systems by the Juvenile Probation Department, 7) Computer Management System by the Library, and 8) Social Media Monitoring Software by the Library; and making required findings in support of said approvals.

Background Information

Chapter 19B regulates City Departments' acquisition and use of Surveillance Technology.

Under 19B.5, City Departments that possessed or were using Surveillance Technology before Chapter 19B took effect in July 2019 must obtain Board of Supervisors approval by ordinance of a Surveillance Policy for each type of existing Surveillance Technology.

Under Chapter 19B.2, a Department must obtain Board of Supervisors approval by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Surveillance Technology Policy ordinance approved by the Board in accordance with Chapter 19B; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering into an oral or written agreement under which a non-City entity or individual regularly provides the Department with data or information acquired through the entity's use of Surveillance Technology.

Beginning in August 2019, Departments submitted to the Committee on Information Technology ("COIT") inventories of their existing Surveillance Technology and submitted Surveillance Impact Reports for each type of Surveillance Technology on their inventory. After receiving the inventories and Surveillance Impact Reports, COIT and its Privacy and Surveillance Advisory Board ("PSAB") subcommittee, conducted multiple public hearings, at which COIT and PSAB considered both the inventories and Surveillance Impact Reports for existing Surveillance Technology. Following those hearings, COIT developed Surveillance

Technology Policies for multiple Departments covering seven categories of Surveillance Technology:

(1) Automatic License Plate Readers (ALPR)
(2) Biometric Processing Software or System
(3) Body-Worn Cameras
(4) People-Counting Camera
(5) Third-Party Security Cameras; and
(6) Location Management System.
(7) Computer Management System

Additionally, the Library submitted a Surveillance Impact Report for Social Media Monitoring Software. Based on the Surveillance Impact Reports, COIT developed a Surveillance Technology Policy for Social Media Monitoring Platforms used by the Library.

The Surveillance Technology Policies that COIT developed for each Department are detailed in Sections 2 through 9 of the proposed ordinance. The Surveillance Technology Policies are available in Board File No. 220843. COIT recommends that the Board of Supervisors approve each Surveillance Technology Policy.

n:\govern\as2022\1900636\01632429.docx

City & County of San Francisco
London N. Breed, Mayor

Office of the City Administrator
Carmen Chu, City Administrator
Jillian Johnson, Director
Committee on Information Technology

To: Angela Calvillo
Clerk of Board of Supervisors

From: Carmen Chu, City Administrator
Jillian Johnson, Director, Committee of Information Technology

Date: July 18, 2022

Subject: Legislation introduced for Approval of Surveillance Technology Policies for Multiple City Departments

---

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit Surveillance Technology Policies and Impact Reports for the following technologies to the Board of Supervisors for their review:

- Automatic License Plate Readers (ALPR)
- Biometric Processing Software and/or System
- Body-Worn Cameras
- People-Counting Camera
- Security Cameras
- Third-Party Security Cameras
- Location Management System
- Computer Management System
- Social Media Monitoring Software

The Committee on Information Technology (COIT) and its subcommittee, the Privacy and Surveillance Advisory Board (PSAB), held public meetings over the course of the last year to engage the public in developing these Surveillance Technology policies. All details of these discussions are available at sf.gov/COIT.

The following sections provide more detail on the departments seeking Board of Supervisors approval for their surveillance technology policies, and the COIT recommended course of action.

If you have questions on the review process, please direct questions to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Automatic License Plate Readers (ALPR)

Department	Authorized Uses
Municipal Transportation Agency (MTA)	1. Enforce parking restrictions and laws. 2. Transit Only Lane Enforcement (TOLE). 3. Link individual vehicles to their times of entry/exit into City-owned parking garages and lots to accurately calculate parking fees. 4. Identify vehicles that are the subject of an active investigation by the SFPD (e.g., vehicles included on "hot lists" generated by the SFPD –see Appendix B & C of MTA policy, and page 8 of SFPD ALPR Policy). 5. Analysis of and reporting on parking and curb usage.

ALPR Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
September 24, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the ALPR Surveillance Technology Policy for the MTA.

Biometric Processing Software or System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on continuous alcohol monitoring (CAM) in San Francisco with a court order. The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing. CAM data is analyzed on a daily basis by probation officers to ensure compliance with the Court's order.

Biometric Processing Software/System Public Meeting Dates:

Date	Meeting
January 14, 2022	Privacy and Surveillance Advisory Board (PSAB)
February 17, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Biometric Processing System Surveillance Technology Policy for Juvenile Probation.

Body-Worn Cameras

Departments	Authorized Uses
Fire	- Use by Public Information Officer (PIO) at large incidents to capture video of surroundings and the totality of the incident
Recreation and Parks	- Recording video and audio footage in the event of an incident. Incidents can be: o Actual or potential criminal conduct o Situation when a Park Ranger reasonably believes recordings of evidentiary value may be obtained o Calls for service involving a crime where the recording may aid in the apprehension/ prosecution of a suspect - Providing recording to law enforcement or other authorized persons upon request.

Body-Worn Cameras Public Meeting Dates:

Date	Meeting	Departments
September 10, 2021	PSAB	Fire
September 24, 2021	PSAB	Recreation and Parks
October 21, 2021	COIT	Fire, Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Body-Worn Camera Surveillance Technology Policies for the Fire Department and the Recreation and Parks Department.

People-Counting Cameras

Departments	Authorized Uses
Library	- To tally the entry and exit of Library visitors at all 28 public facilities. - To track usage of meeting rooms, elevators and restrooms for purposes of resource allocation.

People-Counting Cameras Public Meeting Dates:

Date	Meeting
January 28, 2022	Privacy and Surveillance Advisory Board (PSAB)
March 11, 2022	Privacy and Surveillance Advisory Board (PSAB)
April 21, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the People-Counting Camera Surveillance Technology policy for the Library.

Security Cameras

Departments	Authorized Uses
Elections	- Live monitoring of voting center lines. - Live monitoring of Department staff during elections operations. - Recording of video and images of Department staff during elections operations. - Reviewing camera footage of Department staff in the event of an incident. - Sharing camera footage of Department staff with the public to promote transparency into elections operations.

Security Cameras Public Meeting Dates:

Date	Meeting
October 22, 2021	Privacy and Surveillance Advisory Board (PSAB)
November 18, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Security Camera Surveillance Technology Policy for the Department of Elections.

Third-Party Security Cameras

Departments	Authorized Uses
Airport (AIR)	- Reviewing camera footage in the event of an incident. - Approving Tenant's disclosure of digital recordings and other data from its security camera system.
Municipal Transportation Agency (MTA)	- Review recording of on-board incidents based upon complaints received from the public and at appeals hearing in response to a fine, suspension or response to fine revocation. - Review video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transportation Code. - Review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides. For example, under its wheelchair program taxi incentive, the Department reviews video data from the technology to confirm that taxi cab drivers pick up individuals with certain disabilities before paying drivers for those rides, which are funded under various paratransit programs. - Review video to investigate criminal acts involving taxi drivers or riders. - Review video data to investigate accidents involving a taxi cab.
War Memorial (WAR)	- Live monitoring internal office space and public area of Davies Symphony Hall. - Reviewing camera footage provided by Tenant/Contractor upon request in the event of an incident.

Third-Party Security Cameras Public Meeting Dates:

Date	Meeting	Departments
October 22, 2021	PSAB	WAR
January 14, 2022	PSAB	WAR, AIR
January 28, 2022	PSAB	AIR
February 17, 2022	COIT	AIR
March 11, 2022	PSAB	MTA
April 21, 2022	COIT	WAR, MTA

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Third-Party Security Camera Surveillance Technology Policies for the Airport, Municipal Transportation Agency, and War Memorial.

Location Management System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on electronic monitoring in San Francisco with a court order. The Court may order a youth to be placed on electronic monitoring as an alternative to detention. - Electronic monitoring (EM) may also be added as a condition of probation if additional supervision is warranted. EM data is analyzed on a daily basis by probation officers to ensure compliance with: - Court ordered curfews o Inclusion zones: addresses/areas where the minor has approval to be present, for example their home, school, work. o Exclusion zones: addresses/areas where the minor should not be present, including Stay Away orders o Schedules: To monitor school attendance, program participation, work.
Recreation and Parks	- Confirm that the person who reserved the booking for a tennis court is at the location at the reserved time. - Utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time.

Location Management System Public Meeting Dates:

Date	Meeting	Department
October 22, 2021	PSAB	Juvenile Probation
November 18, 2021	COIT	Juvenile Probation
March 11, 2022	PSAB	Recreation and Parks
May 27, 2022	PSAB	Recreation and Parks
June 16, 2022	COIT	Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Location Management Surveillance Technology Policies for Juvenile Probation and the Recreation and Parks Department.

Social Media Monitoring Software

Department	Authorized Uses
Library	- Plan and execute more effective and strategic campaigns across social media platforms. - Schedule multiple social media posts in advance. - Create and monitor multiple streams of content across various platforms. - Maintain active social media presence that is automated, specifically on weekends when staff is off. - Ensure consistency of messaging across all social media platforms. - Track post performance and analyze trends to improve content and strategy. - Create reports.

Social Media Monitoring Software Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Social Media Monitoring Software Surveillance Technology Policy for the Library.

Computer Management System

Departments	Authorized Uses
Library	- The authorized use case for the TBS Computer Time and Print Management tool is to provide time-delimited public access to library computers and allow the public to print, copy, scan and fax documents, as well as track usage of computers and print resources throughout the library's 28 facilities for purposes of resource allocation and management.The five specific components within TBS Computer Time and Print Management are as follows: • MyPC: Manages patron access to library computers and regulates amount of time each patron can use computers • EZ Booking: Allows patrons to manage their reservations in MyPC, schedule public computer use, etc. • Papercut/EPrintIt: Manages public print jobs sent from library computers and patrons' personal devices, allowing them to print their documents on library printers. Also allows select library staff members, in the interest of customer service and support, to retrieve and print jobs submitted to the system by users during the 24-hour period in which documents are retrievable. This allows staff to print jobs when printers fail, when print jobs do not meet user expectations, to intermediate when users are struggling with technology, etc. • Allows library patrons to scan, manipulate, manage, print, email, fax and save documents using either the library's flat-bed or document feeder scanners. • Payment Kiosk: Allows patrons to pay for print and copy jobs processed through Papercut/EPrintIt and/or ScanEZ.

Security Cameras Public Meeting Dates:

Date	Meeting
May 27, 2022	Privacy and Surveillance Advisory Board (PSAB)

June 16, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Computer Management System Surveillance Technology Policy for the Library.

Surveillance Impact Report

San Francisco International Airport ("Airport" or "Department")
Tenant Security Cameras

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the San Francisco International Airport ("Airport" or "Department") use of digital recordings and data from third party security cameras.

DESCRIPTION OF THE TECHNOLOGY

This impact assessment applies to the Airport's access to and use of digital recordings and other data from and the security cameras of the following entities:

- Airport airlines, concessionaires, food and beverage operators, and rental car agency tenants. ("Tenants")

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Reviewing camera footage in the event of an incident.
2. Approving Tenant's disclosure of digital recordings and other data from its security camera system.

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

Further, processing of personal data revealing 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.

Tenants' technology may be deployed in the following locations, based on use case:

Tenants' proprietary lease space.

Surveillance Oversight Review Dates
COIT Review: TBD
Board of Supervisors Review: TBD

Technology Details

The following a is product description:

There are various types of camera technology used by the Tenants. During the application process Tenants are required to provide the Airport with camera make, model, and technical specifications as well as their security plan. Tenants are responsible for their hardware and the Airport does not maintain an inventory except as noted on the Tenants application form. Tenants are required to update the Airport on their inventory as change occurs.

A. How It Works

Subject to the Airport Rules and Regulations, Tenants are allowed to install their own security cameras in their proprietary lease space. Tenants use these cameras to record live video within their proprietary lease space.

Handling or storage of data collected from or processed by Tenant's security camera system is solely the responsibility of Tenant.

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: - One year, consistent with the Department's Data Retention Policy and state law; longer if necessary for an ongoing investigation or in anticipation of litigation. 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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s): - If necessary for an ongoing investigation or in anticipation of litigation. 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.) ▪ Department of Technology Data Center ▪ 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:

Practices:

- 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.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Tenant's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Tenants use of security cameras has the following benefits for the residents of the City and County of San Francisco:

▪	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	
▪	Other	

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

Airport's use of recordings and data from third party security cameras is restricted to the identified Authorized Use Cases. Tenant's disclosure of recordings and data from its own cameras is subject to the Airport Rules and Regulations and policies that restrict use of CCTV to the approved use in the Tenant Application. Tenants are required to report to the Airport any changes or modifications to video monitoring and/or recording device use prior to executing the changes or modifications.

Tenants are required to obtain Airport's written authorization prior to the release of any video monitoring and/or recording device footage from Tenants cameras/devices. In appropriate cases, Airport may also request review and a determination of whether the footage may be disclosed from the Transportation Security Administration (TSA).

Further, Tenants approved camera use are audited as part of the Airport weekly and monthly audit of Tenants space. Airlines are also audited on an annual basis.

C. Fiscal Analysis of Costs and Benefits

The Department's use of surveillance cameras yields the following business and operations benefits [Please customize chart below according to department circumstances]:

Benefit		**Description**
X	Financial Savings	Tenants security Camera Systems will save on building or patrol officers.
X	Time Savings	Tenants security Camera Systems will run 24/7/365, thus decreasing or eliminating building or patrol officer supervision.
X	Staff Safety	Tenants security cameras help identify violations 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 recommended to be set to high resolution.

Number of FTE (new & existing)	Tenants cost to implement and support security cameras are not reported to Airport. Cost noted in this table reflect the Airport's cost for the approval and audit of Tenants use of the technology. .45	
Classification	1. 9212 – Aviation Security Analyst – 10% 2. 9220 – Aviation Security Supervisor – 10% 3. 0931 – Manager Aviation Security & Regulatory Compliance – 10% 4. 0933 - Director, Security, Emergency Management & Communications – 10% 5. 0943 - Managing Director, Safety, Security and Airside Services – 5% 6. 0955 – Chief Operating Officer – 5%	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment		
Professional Services		
Training		
Other – Salaries & Benefits	$ 108,000	
Total Cost	**$ 108,000**	

The Department funds its use and maintenance of the surveillance technology through

Annual Operating funds. Tenants fund their use and maintenance of the surveillance technology.

COMPARISON TO OTHER JURISDICTIONS

Third Party Security Cameras are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Mapped Crime Statistics

The general location(s) it may be deployed and crime statistics for any location(s):

Tenants proprietary space across the Airport property.

Surveillance Technology Policy

Tenant Security Cameras
SAN FRANCISCO INTERNATIONAL AIRPORT ("SFO", "Airport", OR "Department")

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, this Surveillance Technology Policy aims to ensure the responsible use of Security Camera Systems by airlines, concessionaires, food and beverage operators, rental car agency tenants (hereinafter Tenants) at the San Francisco Internal Airport ("SFO", "Airport", OR "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 provide an exceptional airport in service to our communities.

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, and other agents acting on the Department's behalf that access or use digital recordings or other data from Tenants Security Camera Systems, including employees, contractors, and volunteers.

POLICY STATEMENT

This policy applies to the Airport's access to and use of digital recordings and other data from the security cameras of the following entities:

- Airport Tenants

The Airport limits its use of recordings and other data from Tenant security cameras to the following authorized use cases and requirements listed in this Policy only.

Authorized Use(s):

1. Reviewing camera footage in the event of an incident.
2. Approving Tenant's disclosure of digital recordings and other data from its security camera system.

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.

Surveillance Oversight Review Dates
COIT Review: February 17, 2022
Board of Supervisors Review: Upcoming

BUSINESS JUSTIFICATION

Access to and use of digital recordings and other data from Tenant Security cameras will benefit the Department in the following ways.:

	▪ 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	

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Equipment is owned and operated by non-city entity.
X	Time Savings	Tenant/Contractor Security Camera Systems operate 24/7/365, thus decreasing or eliminating building or patrol officer supervision. Additionally, full-time staffing is not required to subsequently review footage of security incidents.
X	Staff Safety	Tenant/Contractor Security cameras help identify violations of 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.

- Service Levels

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 the data that is necessary to execute the authorized use cases. All surveillance technology data shared with Department by a 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

Access:

The Airport does not have direct system access to, or control over, the operation of Tenant's technology. Recorded footage is accessed only in response to an incident.

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:

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0931 – Manager Aviation Security & Regulatory Compliance.
- 0933 - Director, Security, Emergency Management & Communications
- 0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

The following providers are required to support and maintain the surveillance technology and its associated data to ensure it remains functional:

- Tenants/Vendors are responsible for the maintenance of the surveillance technology systems.

B. Members of the public

	Data collected by surveillance technology will not be made generally available to members of the public. 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.
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 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. - 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 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:	Tenant/Contractor is the sole owner and custodian of its Surveillance Technology data. Tenant/Contractor may share such data with the Department, but pursuant

to Airport Rule & Regulation 7.5, must seek prior authorization from Department for release to other third parties.

The Department will endeavor to ensure that other agencies or departments that may receive data collected by Tenant's security cameras will act in conformity with this Surveillance Technology Policy.

In the event of a substantive amendment to Rule 7.5, the Department must resubmit this Policy for approval in accordance with Chapter 19B.

Data is shared by Tenant/Contractor with the Department as needed.

A. Internal Data Sharing

In the event of an incident, Security Camera images may be shared with the following agencies:

- Within the Department on a need-to-know basis
- Police
- City Attorney
- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other law enforcement agencies
- Member(s) of the public, if required under the California Public Records Act or the Sunshine Ordinance

Data sharing occurs at the following frequency:

- As needed.

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: - One year, consistent with the Department's Data Retention Policy and state law; longer if necessary for an ongoing investigation or in anticipation of litigation. 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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s): - If necessary for an ongoing investigation or in anticipation of litigation. 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.) ▪ Department of Technology Data Center ▪ 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: - 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 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 memoranda of understanding with the labor organization representing employees of the City and County of San Francisco.

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.

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

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0931 – Manager Aviation Security & Regulatory Compliance.

- 0933 - Director, Security, Emergency Management & Communications
- 0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

DEFINITIONS	
Tenant/Contractor	Non-City Entity that owns and operates security cameras and shares security camera footage with a City department.
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."

QUESTIONS & CONCERNS

Public:

Complaints, concerns or questions can be submitted to:

- *Airport Guest Services - https://www.flysfo.com/contact-sfo(Contact SFO)*
- *Airport public email, phone, or website --https://www.flysfo.com/contact-sfo or*
- *Airport Commission meetings -- https://www.flysfo.com/about-sfo/airport-commission/addressing-the-commission*

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall follow its process where questions and complaints are tracked by Airport Guest Services and response are promptly responded to by the Director of Guest Experience and/or his staff.

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.

Attachment 1: Appendix A: Rules and Regulations, Rule 7.5 (2022 edition)

RULE 7.0

AIRPORT SECURITY

7.5 VIDEO MONITORING AND RECORDING DEVICES / ACCESS TO AIRPORT CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM

(A) Installation or Removal of Video Monitoring and Other Recording Devices

No video monitoring or other recording devices may be installed or removed by any Airport tenant or contractor in or around the Airport premises without prior written authorization from the Aviation Security unit. To obtain authorization for CCTV camera installation or removal, tenants and contractors must submit an application, specifying the following:

- Field-of View (FOV) screenshots
- Video monitoring/recording device model and specifications
- Recording system and retention time
- Camera layout drawing
- Security infrastructure and plan to prevent unauthorized access

The use of Pan-Tilt-Zoom (PTZ) security cameras by tenants and contractors in any Restricted area is strictly prohibited and no video monitoring and/or recording device may be installed or focused in a manner that depicts/records security checkpoints, or doors that provide access to any area on Airport premises that, in the sole and exclusive discretion of the Director or his designee, is deemed to present a potential risk to Airport security. All subsequent changes or modifications to tenant and contractor video monitoring and/or recording device use must be submitted to Aviation Security in writing and approved prior to executing modifications.

(B) Remote Viewing and Authorization Access

No video monitoring and/or recording device data may be streamed or otherwise transmitted on a wireless network unless the wireless network is equipped with WPA2 security. Real-time access to all footage must be available to the Aviation Security unit at all times. No tenant or contractor shall release any video monitoring and/or recording device footage from cameras/devices without prior written authorization from the Aviation Security unit and, if deemed appropriate, the TSA. Remote access to video monitoring and/or recording devices in secure areas will not be permitted unless explicitly authorized by the Director.

All forms of video footage, whether real-time or stored, must be password protected. Passwords must comply with the Airport's Password policy.

(C) Inventory of Video Monitoring and Other Recording Devices

All tenants and contractors shall provide Aviation Security with an inventory of existing video monitoring and/or recording devices and security plans, including all of the following:

- Device manufacturer, model and specifications
- Field-of-view
- Data retention time
- Placement of video monitoring and/or recording devices

- Remote access usage
- Written security plan detailing how unauthorized access will be prevented

(C) Airport Closed-Circuit Television (CCTV) Access Policy

The Airport owns and operates the CCTV system. This system contains information that is confidential, which may be sensitive secure, affect personal privacy, or both. A tenant or contractor may access Airport CCTV feeds only through Airport equipment upon request to Airport Aviation Security (AVSEC). If access is granted, the tenant or contractor shall designate individual employees to view CCTV feeds for the performance of official job duties, on a need-to-know basis only. Any such individual must hold an Airport ID badge and execute a Non-Disclosure Acknowledgement as a condition of authorized access. (ASB 20-02, ASB 20-06)

Surveillance Impact Report

Body-Worn Cameras
Fire Department

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of body-worn cameras.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to protect the lives and property of the people of San Francisco and its visitors from fires, natural disasters, accidents, hazardous materials incidents, and other causes requiring a rapid and skilled response by land or water; serve the needs of its most vulnerable residents through community paramedicine, and save lives and reduce suffering by providing emergency medical services; prevent harm through prevention services and education programs; and to provide a work environment that is free from harassment and discrimination, and values health, wellness, cultural diversity, and equity.

In line with its mission, the Department uses body-worn cameras. This technology is a tool used by Department staff in front-line operational response, to improve aspects of the Department (such as training) that directly support the mission statement.

The Department shall use body-worn cameras only for the following authorized purposes:

- Use by Public Information Officer (PIO) at large incidents to capture video of surroundings and the totality of the incident (currently in use).

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is located or generally deployed to any large scale emergency event in San Francisco.

Surveillance Oversight Review Dates
COIT Review: October 21, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description of body-worn cameras:

Axon Flex 2 brings point-of-view video to the next level, with a rugged design, a range of mounts and advanced capabilities like unlimited HD and a 120-degree field of view.

How It Works

To function, body-worn cameras are worn by the SFFD member to capture video. It is turned off and on solely by the member when he arrives on-scene.

All data collected or processed by body-worn cameras will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by Axon to ensure the Department may continue to use the technology.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of Body-Worn Cameras has the following benefits for the residents of the City and County of San Francisco:

- Public Safety: The Department can review incidents for ways to improve response or training opportunities, which then can improve overall emergency response.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

- The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:
    - The San Francisco Fire Department strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures. The Fire Department intends to use body-worn cameras and their associated data

exclusively for aforementioned authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

- To protect camera data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure servers. Only persons authorized to utilize the raw data may access the information
- Only data that has been edited to remove PII will be shared and stored on servers, and sharing will only occur with partner CCSF agencies on a case by case basis or as required by law. To mitigate any potential impacts to residents' physical safety or economic loss through property damage
- Recorded data will not be collected, disseminated or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations). Collection, use, dissemination, or retention of recorded data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of the law.

- Administrative Safeguards: The vendor has a number of technical safeguards in place that are discussed in the section for technical safeguards. For the Department, as a policy we have limited the users that have any access to this system, currently limited to one IT staff and our Public Information Officer. This technology and purpose has been folded into the Department's social media policy, which is enforced and reviewed with any personnel that would have access to this information. Informal training on PII and redaction are done initially and on an as-needed basis to refresh rules and requirements pertaining to PII.
- Technical Safeguards: Data is securely stored on the vendor's cloud site, where access is extremely limited by the Department. There are currently two authorized users for the account. Video is encrypted in transit and while in storage. In transit it is FIPS 140-2 validated, and the system is fully CJIS compliant. There are expanded audit trails for chain of custody and time stamps built into the system.
- Physical Safeguards: Physical camera hardware is secured by member assigned to it and is worn when in operation. There is no physical protection from the uploaded data, as it is stored remotely on a cloud server.

C. Fiscal Analysis of Costs and Benefits

The Department's use of body-worn cameras yields the following business and operations benefits:

- Potential Training Opportunities: Department staff could review video from an incident as part of an after-action review to give points and potential training points for future response improvements.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing):

    - One H-20 Lieutenant
    - One 1070 Project Manager
- The annual costs are:
    - Total Salary & Fringe: 0
    - Software: $2000.00
    - Hardware/ Equipment: 0
    - Professional Services: 0
    - Training: 0
    - Other: 0

The Department funds its use and maintenance of the surveillance technology through the general fund.

COMPARISON TO OTHER JURISDICTIONS

Body-worn cameras are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Body-Worn Cameras
San Francisco Fire Department

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 body-worn cameras itself as well as any associated data by the San Francisco Fire Department ("Fire Department", "SFFD", OR "Department"), and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Fire Department's mission is to protect the lives and property of the people of San Francisco and its visitors from fires, natural disasters, accidents, hazardous materials incidents, and other causes requiring a rapid and skilled response by land or water; serve the needs of its most vulnerable residents through community paramedicine, and save lives and reduce suffering by providing emergency medical services; prevent harm through prevention services and education programs; and to provide a work environment that is free from harassment and discrimination, and values health, wellness, cultural diversity, and equity.

The Surveillance Technology Policy ("Policy") defines the manner in which the body-worn cameras 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 body-worn cameras, 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 body-worn camera technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Use by Public Information Officer (PIO) at large incidents to capture video of surroundings and the totality of the incident, and to review incident response to inform training and make improvements to future incident response.

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

Departments 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. 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

Body-worn cameras support the Department's mission and provides important operational value in the following ways:

This technology is a tool used by Department staff in front-line operational response, to improve aspects of the Department (such as training) that directly support the mission statement.

In addition, body-worn cameras promise to benefit residents in the following ways:

- Public Safety: The Department can review incidents for ways to improve response or training opportunities, which then can improve overall emergency response.

Body-worn cameras will benefit the department in the following ways:

- Potential Training Opportunities: Department staff could review video from an incident as part of an after-action review to give points and potential training points for future response improvements.

To achieve its intended purpose, body-worn cameras (hereinafter referred to as "surveillance technology") is worn by the SFFD member to capture video. It is turned off and on solely by the member when they arrive on-scene.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- Classified Data Types: Faces or license plates - While it is intended to only capture the scene of a fire, there may inadvertently be faces, license plates, or other visual PII captured on video.
- Data Format: MOV, AVI
- Data Security Classification: Level 2

Access: All parties requesting access must adhere to the following rules and processes (please refer the data sharing section to ensure all information covered in that section is also included below):

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:

- H-20 Lieutenant (1)
- 1070 IS Project Manager (1)

Access to data is limited to Department PIO and IT manager. Data must always be scrubbed of PII prior to sharing beyond these authorized roles.

B. Members of the public, including criminal defendants

The Fire 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

Access to data is limited to the SFFD PIO and a Department IT manager. Data is stored remotely on vendor's cloud servers, and would be scrubbed of PII if shared beyond authorized roles. Video is encrypted in transit and while in storage.

Data Sharing: The Fire Department will endeavor to ensure that other agencies or departments that may receive data collected by the Fire Department's Body-Worn Cameras 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.

The Fire 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)

The Fire Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Fire 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 currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share unredacted surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing

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

Before data sharing with any recipient, 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.
- Evaluate what data can be permissibly shared with members of the public should a request be made in accordance with San Francisco's Sunshine Ordinance.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	**Retention Justification**

Data is currently stored indefinitely as SFFD works to update its internal data retention policy. Data retention period shall match Department's internal data retention policy once updated.	Video data is stored indefinitely given the low volume of data and extremely limited access. Video is scrubbed of PII if shared beyond authorized roles. Department is updating its internal data retention policy, which will be informed in part by State mandates.

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.

Data will be stored in the following location:

- Cloud Storage Provider: Data is securely automatically uploaded to a cloud server, where it can be accessed.

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- Due to the small volume of data relative to other data, video is currently stored indefinitely on the vendor's server. The Department is currently working on an update to its data retention policy.

Processes and Applications:

- The vendor has a redaction assistant built into its software to assist with removal/blurring of PII. This specifically covers screens, faces and license plates automatically

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.

At the very least, 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. 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.

- Access is extremely limited, currently with two members. If a new SFFD member were to be granted access they would be trained on using the vendor's system. This training would encompass accessing the vendor's system, as well as viewing and retrieving videos. Department members granted access are currently given Department training on the needs for removing PII in general.

In addition, this technology has previously fallen under the Department's social media policy, so a review of that policy is required.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

Department shall assign the following personnel to oversee Policy compliance by the Department and third parties: Supervisor- Management of Information Services

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

- 1070 IS Project Director
- 0941 Manager VI

Sanctions for violations of this Policy include the following:

- First offense: violator shall be verbally notified by Fire Department management of nature of violation.
- Second offense: violator shall be notified in writing of second offense and privileges to operate body-cam hardware shall be suspended for 60 days.
- Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from body cam operations and disciplinary action may be taken depending upon the severity of second/third offences.

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:

Department Members or the general public can register complaints/concerns or submit questions via calls or service requests to San Francisco 311 Customer Service Center, or to the Department directly at FireAdministration@sfgov.org or 415-558-3200.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- Constituent calls and complaints to the Fire Department are routed to the appropriate Program manager.
- Program manager will discuss concerns or complaints with constituent and record details regarding nature of conversation.
- If additional action is required or requested by caller, the Fire Department commits to a follow-up (by email or telephone) in a timely manner.
- Program Manager, body-worn camera operators, and Fire Department management shall review log of complaints on a quarterly basis to discuss best practices. Department will evaluate caller complaints, concerns and other community feedback for learning lessons and opportunities to improve the body camera use program.

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.

Surveillance Impact Report

SCRAM GPS

Juvenile Probation Department

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of SCRAM GPS Ankle Monitor Bracelet.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to serve the needs of youth and families who are brought to our attention with care and compassion; to identify and respond to the individual risks and needs presented by each youth; to engage fiscally sound and culturally competent strategies that promote the best interests of the youth; to provide victims with opportunities for restoration; to identify and utilize the least restrictive interventions and placements that do not compromise public safety; to hold youth accountable for their actions while providing them with opportunities and assisting them to develop new skills and competencies; and contribute to the overall quality of life for the citizens of San Francisco within the sound framework of public safety as outlined in the Welfare & Institutions Code.

In line with its mission, the Department uses SCRAM GPS Ankle Monitor Bracelet to:

Electronic monitoring, as ordered by the Court, is used as an alternative to detention or as a measure of stepped up supervision for youth on probation, supporting the Department's mission to respond to individual risks and needs, engage in fiscally sound strategies that promote the best interest of youth, support victims, and to utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

The Department shall use SCRAM GPS Ankle Monitor Bracelet only for the following authorized purposes:

- Youth are only placed on electronic monitoring in San Francisco with a court order. The Court may order a youth to be placed on electronic monitoring as an alternative to detention.
- Electronic monitoring (EM) may also be added as a condition of probation if additional supervision is warranted. EM data is analyzed on a daily basis by probation officers to ensure compliance with:
    - Court ordered curfews
    - Inclusion zones: addresses/areas where the minor has approval to be present, for example their home, school, work.
    - Exclusion zones: addresses/areas where the minor should not be present, including Stay Away orders
    - Schedules: To monitor school attendance, program participation, work.

Surveillance Oversight Review Dates

COIT Review: November 18, 2021

Board of Supervisors Review: TBD

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is located in San Francisco and the Bay Area.

Technology Details
The following is a product description of SCRAM GPS Ankle Monitor Bracelet:

Continuously signaling, or "active" Electronic Monitoring systems have three essential parts: a transmitter, a receiver/dialer and a central computer. The transmitter is strapped to the participant and broadcasts a coded signal over a telephone line at regular intervals. The receiver/dialer picks up signals from the participant's transmitter and reports to a central computer when the signals stop and start. The computer compares any signal interruptions with the participant's curfew schedule (inconsistent, pre-determined movement or geographical locations) and alerts correctional officials to unauthorized absences.

A. How It Works

To function, SCRAM GPS Ankle Monitor Bracelet consists of placing FCC-certified ankle bracelets on participants that monitor location through global positioning system (GPS) technology. The bracelets are placed in such a way that they cannot be removed. At least once per minute, 24 hours per day, 7 days per week, the bracelet transmits location information via the cellular network to a central computer. The information is compared with the court ordered curfew schedule and/or inclusion/exclusions zones. SCRAM provides a web-based interface for JPD to access the monitoring data.

All data collected or processed by SCRAM GPS Ankle Monitor Bracelet will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by SCRAM of California to ensure the Department may continue to use the technology.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of SCRAM GPS Ankle Monitor Bracelet has the following benefits for the residents of the City and County of San Francisco:

- Criminal Justice, Public Safety: Electronic monitoring enables the Court to utilize the least restrictive intervention to respond to juvenile delinquency and promote public safety. This technology benefits residents by safely reducing the detention of youth in juvenile hall and advancing community safety.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

- Risks and Mitigation: The Department has considered the potential civil rights/liberties impacts associated with the surveillance technology and has identified administrative, technical, and physical safeguards to mitigate these impacts through responsible technology and data use policies and procedures. JPD utilizes SCRAM electronic monitoring only as ordered by the Court for authorized use cases. All other uses are expressly prohibited.
- Administrative Safeguards: All sworn Probation Services Personnel are provided training by SCRAM on how to install, removed, activate, and deactivate, an Electronic Monitor, as well as being able to navigate the SCRAM web-based interface prior to using the system prior to accessing or using the technology. The Director of Probation Services or designee will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Probation Services. All sworn Probation Services personnel will be trained on the Surveillance Technology policy. Violation of the policy will be subject to standard JPD departmental policies, which may include disciplinary action up to and including termination.
- Technical Safeguards: TLS for transmission, encrypted at rest; security measures that allow only authorized personnel to access.
- Physical Safeguards: Hardware is stored in locked office.

C. Fiscal Analysis of Costs and Benefits

The Department's use of SCRAM GPS Ankle Monitor Bracelet yields the following business and operations benefits:

- Improved Data Quality, Time Savings: Electronic monitoring benefits department operations by providing alternatives to detention pursuant to the order of the Court in a manner that is responsive to individual risks and needs, and by engaging in fiscally sound strategies that promote the best interest of youth, support victims, utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): Technical support is provided by SCRAM.
- The annual costs are:
    - Total Salary & Fringe: 0
    - Software: 0
    - Hardware/ Equipment: 0
    - Professional Services: $84,489.84
    - Training: 0
    - Other: 0

The Department funds its use and maintenance of the surveillance technology through

Juvenile justice apportionments from the state are the source of funding for the technology.

COMPARISON TO OTHER JURISDICTIONS

SCRAM GPS Ankle Monitor Bracelets are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

SCRAM Global Positioning System (SCRAM GPS)
Juvenile Probation Department

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 SCRAM Global Positioning System ("SCRAM GPS") itself as well as any associated data by the Juvenile Probation Department ("Department"), and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Juvenile Probation Department's mission is to serve the needs of youth and families who are brought to our attention with care and compassion; to identify and respond to the individual risks and needs presented by each youth; to engage fiscally sound and culturally competent strategies that promote the best interests of the youth; to provide victims with opportunities for restoration; to identify and utilize the least restrictive interventions and placements that do not compromise public safety; to hold youth accountable for their actions while providing them with opportunities and assisting them to develop new skills and competencies; and contribute to the overall quality of life for the citizens of San Francisco within the sound framework of public safety as outlined in the Welfare & Institutions Code.

The Surveillance Technology Policy ("Policy") defines the manner in which SCRAM GPS will be used to support this mission, by describing the 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 SCRAM GPS, 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 SCRAM GPS technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Youth are only placed on electronic monitoring in San Francisco with a court order. The Court may order a youth to be placed on electronic monitoring as an alternative to detention.
- Electronic monitoring (EM) may also be added as a condition of probation if additional supervision is warranted. EM data is analyzed on a daily basis by probation officers to ensure compliance with:
    - Court ordered curfews

- Inclusion zones: addresses/areas where the minor has approval to be present, for example their home, school, work.
- Exclusion zones: addresses/areas where the minor should not be present, including Stay Away orders
- Schedules: To monitor school attendance, program participation, work.

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

Departments 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. 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

SCRAM GPS supports the Department's mission and provides important operational value in the following ways:

Electronic monitoring, as ordered by the Court, is used as an alternative to detention or as a measure of stepped up supervision for youth on probation, supporting the Department's mission to respond to individual risks and needs, engage in fiscally sound strategies that promote the best interest of youth, support victims, and to utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

In addition, SCRAM GPS promises to benefit residents in the following ways:

- Criminal Justice, Public Safety: Electronic monitoring enables the Court to utilize the least restrictive intervention to respond to juvenile delinquency and promote public safety. This technology benefits residents by safely reducing the detention of youth in juvenile hall and advancing community safety.

SCRAM GPS will benefit the department in the following ways:

- Improved Data Quality, Time Savings: Electronic monitoring benefits department operations by providing alternatives to detention pursuant to the order of the Court in a manner that is responsive to individual risks and needs, and by engaging in fiscally sound strategies that promote the best interest of youth, support victims, utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

To achieve its intended purpose, SCRAM GPS (hereinafter referred to as "surveillance technology") consists of placing FCC-certified ankle bracelets on participants that monitor location through global positioning system (GPS) technology. The bracelets are placed in such a way that they cannot be removed. At least once per minute, 24 hours per day, 7 days per week, the bracelet transmits location information via the cellular network to a central computer. The information is compared with the court

ordered curfew schedule and/or inclusion/exclusions zones. SCRAM provides a web-based interface for JPD to access the monitoring data.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- Data Types: Geolocation data (periodic latitude and longitude points)
- Date Format: Stored in binary in a SQL database
- Data Security Classification: Level 4

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:

- Department identification
- Description of the authorized use
- Information on the surveillance technology
- Type of data collected

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Youth are only placed on electronic monitoring in San Francisco with a court order, and Sworn Probation Services Personnel only access or use data pursuant to the court order.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- (21) Class 8444 Deputy Probation Officers
- (6) Class 8434 Supervising Probation Officers
- (1) Senior Supervising Probation Officer
- (1) Director of Probation Services
- (1) Chief Probation Officer

B. Members of the public, including criminal defendants

The Juvenile Probation 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Department shall, at minimum, apply the following safeguards:

The SCRAM GPS web-based interface includes security measures that allow only authorized personnel to access and use the data. SCRAM uses Transport Layer Security (TLS) for transmission, encrypted at rest.

Data Sharing: The Juvenile Probation Department will endeavor to ensure that other agencies or departments that may receive data collected by Juvenile Probation Department's SCRAM GPS Policy 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.

The Juvenile Probation 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)

The Juvenile Probation Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Juvenile Probation 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 currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Data Type	Data Recipient
Geolocation data for the individual in question	Data regarding individual youth may be shared on a need to know basis and/or pursuant to a court order with the Police Department, District Attorney, and Public Defender, pursuant to an ongoing investigation and/or court proceeding.

Data sharing occurs at the following frequency:

- On a case-by-case basis.

B. External Data Sharing

Department shares the following data with the recipients:

Data Type	Data Recipient
Geolocation data for the individual in question.	Data regarding individual youth may be shared on a need to know basis and/or pursuant to a court order with the Superior Court, or other Law Enforcement Agencies outside of CCSF, pursuant to an ongoing investigation and/or court proceeding.

Data sharing occurs at the following frequency:

- On a case-by-case basis.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

Data regarding individual youth is only shared on a need to know basis and/or pursuant to a court order with justice system partners who are subject to state laws regarding the confidentiality of juvenile records.

Before data sharing with any recipient, 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.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Data Retention Period	Data Retention Justification
Records are retained pursuant to the schedule defined in the Department Record Retention and Destruction policy, which is guided by state law, depending on the type of case and court orders regarding sealing and destruction. The minimum retention period is 2 years.	Juvenile case file record retention is dictated by state law.

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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Data is retained for the period defined by state law.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- Local storage.

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- When retention period ends, case files are shredded.

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.

At the very least, 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. 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.

- All sworn Probation Services Personnel are provided training by SCRAM on how to install, removed, activate, and deactivate, an Electronic Monitor, as well as being able to navigate the SCRAM web-based interface prior to using the system prior to accessing or using the technology.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Director of Probation Services or designee will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Probation Services. All sworn Probation Services personnel will be trained on the Surveillance Technology policy.

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

The Director of Probation Services (#8416) and the Senior Supervising Probation Officer (# 8415) oversee the Surveillance Technology policy.

Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to standard JPD departmental policies, which may include disciplinary action up to and including termination.

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:

Complaints to the Department are accepted in any format, via any means: phone call, verbal to a staff member, email or by written Complaint Form from the SFJPD website. Members of the public can find more information about how to register complaints on the Department's web site: https://sfgov.org/juvprobation/complaints

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

All complaints are directed to the Chief Probation Officer wherein each complaint is assigned a number, and tracked according to AB-953 by date. A receipt letter is sent to each complainant upon delivery of the complaint to the Chief Probation Officer verifying their complaint has been received. The complaint investigation is then assigned by the Chief Probation Officer to staff who to report back directly to the Chief Probation Officer. Once the complaint has been investigated, a follow-up letter shall be sent to the complainant which includes outcomes from the investigation.

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.

Surveillance Impact Report

SCRAM Continuous Alcohol Monitoring (CAM)
Juvenile Probation Department

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of SCRAM Continuous Alcohol Monitoring (CAM).

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to serve the needs of youth and families who are brought to our attention with care and compassion; to identify and respond to the individual risks and needs presented by each youth; to engage fiscally sound and culturally competent strategies that promote the best interests of the youth; to provide victims with opportunities for restoration; to identify and utilize the least restrictive interventions and placements that do not compromise public safety; to hold youth accountable for their actions while providing them with opportunities and assisting them to develop new skills and competencies; and contribute to the overall quality of life for the citizens of San Francisco within the sound framework of public safety as outlined in the Welfare & Institutions Code.

In line with its mission, the Department uses SCRAM Continuous Alcohol Monitoring (CAM):
Continuous alcohol monitoring (CAM), as ordered by the Court, is used as a measure of stepped up supervision for youth on probation, supporting the Department's mission to respond to individual risks and needs, engage in fiscally sound strategies that promote the best interest of youth, support victims, and to utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

The Department shall use SCRAM Continuous Alcohol Monitoring (CAM) only for the following authorized purposes:

- Youth are only placed on continuous alcohol monitoring (CAM) in San Francisco with a court order. The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing. CAM data is analyzed on a daily basis by probation officers to ensure compliance with the Court's order.

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is located in San Francisco and the Bay Area.

Surveillance Oversight Review Dates
COIT Review: February 17, 2022
Board of Supervisors Review: TBD

Technology Details

The following is a product description of SCRAM Continuous Alcohol Monitoring (CAM):
Like a breathalyzer for the ankle, the SCRAM Continuous Alcohol Monitoring (SCRAM CAM) bracelet provides 24/7 transdermal alcohol testing for hardcore drunk drivers, high-risk alcohol and domestic violence caseloads. By automatically sampling the wearer's perspiration every 30 minutes, the SCRAM CAM bracelet eliminates testing gaps and encourages accountability. SCRAM CAM not only supports sobriety but also results in higher compliance rates with court orders and increases community safety.

A. How It Works

To function, SCRAM Continuous Alcohol Monitoring (CAM) consists of placing FCC-certified ankle bracelets on participants that provide transdermal monitoring of alcohol consumption 24 hours a day, by sampling the wearer's perspiration every thirty minutes. The bracelets are placed in such a way that they cannot be removed. The bracelet transmits transdermal monitoring information via the cellular network to a central computer. SCRAM provides a web-based interface for JPD to access the monitoring data.

All data collected or processed by SCRAM Continuous Alcohol Monitoring (CAM)
will be handled or stored by an outside provider or third-party vendor on an ongoing basis.
Specifically, data will be handled by SCRAM of California to ensure the Department may continue to use the technology.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of SCRAM Continuous Alcohol Monitoring (CAM) has the following benefits for the residents of the City and County of San Francisco:

- Criminal Justice: The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing to abstain from the consumption of alcohol
- Public Safety: Continuous alcohol monitoring (CAM) enables the Court to utilize the least restrictive intervention to respond to juvenile delinquency and promote public safety.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

The Department has considered the potential civil rights/liberties impacts associated with the surveillance technology and has identified administrative, technical, and physical safeguards to mitigate these impacts through responsible technology and data use policies and procedures. JPD utilizes SCRAM continuous alcohol monitoring only as ordered by the Court for authorized use cases. All other uses are expressly prohibited.

Administrative Safeguards: All sworn Probation Services Personnel are provided training by SCRAM on how to install, removed, activate, and deactivate, a Continuous Alcohol Monitor, as well as being able to navigate the SCRAM web-based interface prior to using the system prior to accessing or using the technology. The Director of Probation Services or designee will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policyope for Probation Services. All sworn Probation Services personnel will be trained on the Surveillance Technology policy. Violation of the policy will be subject to standard JPD departmental policies, which may include disciplinary action up to and including termination.

Technical Safeguards: The system used Transport Layer Security (TLS) transmission and is encrypted at rest; the system also includes security measures that allow only authorized personnel to access.

Physical Safeguards: Hardware is stored in locked office.

C. Fiscal Analysis of Costs and Benefits

The Department's use of SCRAM Continuous Alcohol Monitoring (CAM) yields the following business and operations benefits:

- Time Savings: Continuous alcohol monitoring benefits department operations by enabling the Department to ensure compliance with court ordered conditions in a manner that is responsive to individual risks and needs, and by engaging in fiscally sound strategies that promote the best interest of youth, support victims, utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): Technical support is provided by SCRAM.
- The annual costs are:
    - Total Salary & Fringe: 0
    - Software: 0
    - Hardware/ Equipment: 0
    - Professional Services: $5,962
    - Training: 0

- Other: 0

The Department funds its use and maintenance of the surveillance technology through juvenile justice apportionments from the state.

COMPARISON TO OTHER JURISDICTIONS

SCRAM Continuous Alcohol Monitoring (CAM) are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

SCRAM Continuous Alcohol Monitoring (CAM)
Juvenile Probation

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 SCRAM Continuous Alcohol Monitoring (CAM) itself as well as any associated data by the Juvenile Probation Department ("Department"), and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Juvenile Probation Department's mission is to serve the needs of youth and families who are brought to our attention with care and compassion; to identify and respond to the individual risks and needs presented by each youth; to engage fiscally sound and culturally competent strategies that promote the best interests of the youth; to provide victims with opportunities for restoration; to identify and utilize the least restrictive interventions and placements that do not compromise public safety; to hold youth accountable for their actions while providing them with opportunities and assisting them to develop new skills and competencies; and contribute to the overall quality of life for the citizens of San Francisco within the sound framework of public safety as outlined in the Welfare & Institutions Code.

The Surveillance Technology Policy ("Policy") defines the manner in which the SCRAM Continuous Alcohol Monitoring (CAM) 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 SCRAM Continuous Alcohol Monitoring (CAM), 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 SCRAM Continuous Alcohol Monitoring (CAM) technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Youth are only placed on continuous alcohol monitoring (CAM) in San Francisco with a court order. The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing. CAM data is analyzed on a daily basis by probation officers to ensure compliance with the Court's order.

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

COIT Policy Dates
COIT Approved: February 17, 2022
BOS Approved:

Departments 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. 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

SCRAM Continuous Alcohol Monitoring (CAM) supports the Department's mission and provides important operational value in the following ways:

Continuous alcohol monitoring (CAM), as ordered by the Court, is used as a measure of stepped up supervision for youth on probation, supporting the Department's mission to respond to individual risks and needs, engage in fiscally sound strategies that promote the best interest of youth, support victims, and to utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

In addition, SCRAM Continuous Alcohol Monitoring (CAM) promises to benefit residents in the following ways:

- Criminal Justice: The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing to abstain from the consumption of alcohol
- Public Safety: Continuous alcohol monitoring (CAM) enables the Court to utilize the least restrictive intervention to respond to juvenile delinquency and promote public safety.

SCRAM Continuous Alcohol Monitoring (CAM) will benefit the department in the following ways:

- Time Savings: Continuous alcohol monitoring benefits department operations by enabling the Department to ensure compliance with court ordered conditions in a manner that is responsive to individual risks and needs, and by engaging in fiscally sound strategies that promote the best interest of youth, support victims, utilize the least restrictive interventions and placements that do not compromise public safety, and contribute to the quality of life of the citizens of San Francisco.

To achieve its intended purpose, SCRAM Continuous Alcohol Monitoring (CAM) (hereinafter referred to as "surveillance technology") consists of placing FCC-certified ankle bracelets on participants that provide transdermal monitoring of alcohol consumption 24 hours a day, by sampling the wearer's perspiration every thirty minutes. The bracelets are placed in such a way that they can not be removed. The bracelet transmits transdermal monitoring information via the cellular network to a central computer. SCRAM provides a web-based interface for JPD to access the monitoring data.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- Alcohol levels in body, as determined through transdermal readings of perspiration, Level 4 Classification per the City's Data Classification Standard

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.

The department includes the following items in its public notice:

- Department identification
- Description of the authorized use
- Information on the surveillance technology
- Type of data collected.

Data Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Youth are only placed on continuous alcohol monitoring in San Francisco with a court order, and Sworn Probation Services Personnel only access or use data pursuant to the court order.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- All Sworn Probation Services Personnel have access to SCRAM.
- Currently, the personnel include:
  - 21 Class 8444 Deputy Probation Officers
  - 6 Class 8434 Supervising Probation Officers,
  - 1 Senior Supervising Probation Officer
  - 1 Director of Probation Services
  - 1 Chief Probation Officer

B. Members of the public, including criminal defendants

The Juvenile Probation 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

The web-based interface includes security measures that allow only authorized personnel to access and use the data, via unique user name and password.

Data Sharing: The Juvenile Probation Department will endeavor to ensure that other agencies or departments that may receive data collected by JUV's SCRAM Continuous Alcohol Monitoring (CAM) Policy 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.

The Juvenile Probation 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)

The Juvenile Probation Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Juvenile Probation 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 currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Type	**Recipient**
Transdermal alcohol monitoring data for the individual in question.	Data regarding individual youth may be shared on a need to know basis and/or pursuant to a court order with the Police Department, District Attorney, and Public Defender, pursuant to an ongoing investigation and/or court proceeding.

Data sharing occurs at the following frequency:

On a case by case basis.

B. External Data Sharing

Department shares the following data with the recipients:

Type	**Recipient**
Transdermal alcohol monitoring data for the individual in question.	Data regarding individual youth may be shared on a need to know basis and/or pursuant to a court order with the Superior Court, or other Law Enforcement Agencies outside of CCSF, pursuant to an ongoing investigation and/or court proceeding.

Data sharing occurs at the following frequency:

On a case by case basis.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

Data regarding individual youth is only shared on a need to know basis and/or pursuant to a court order with justice system partners who are subject to state laws regarding the confidentiality of juvenile records.

Before data sharing with any recipient, 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.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	**Retention Justification**
Records are retained pursuant to the schedule defined in the Department Record Retention and Destruction policy, which is guided by state law, depending on the type of case and court orders regarding sealing and destruction. The minimum retention period is 2 years	Juvenile case file record retention is dictated by state law, which mandates that records be destroyed or maintained for varying time periods depending on whether a petition was filed, the nature of the sustained offense, whether the record was ordered sealed and/or destroyed by the Court (and the dates so ordered by the Court), and the age of the subject of the petition.

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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Data is retained for the period defined by state law depending on whether a petition was filed, the nature of the sustained offense, whether the record was ordered sealed and/or destroyed by the Court (and the dates so ordered by the Court), and the age of the subject of the petition. See WICs 300, 601, 602, 389, 781, 786, 793, 786.5 and HSC 11357.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- Local Storage
- Software as a Service Product

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- When retention period ends, case files are shredded. When records are sealed, the Department instructs the vendor to remove all identifiers from the data.

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.

At the very least, 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. 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.

All sworn Probation Services Personnel are provided training by SCRAM on how to install, removed, activate, and deactivate, a Continuous Alcohol Monitor, as well as being able to navigate the SCRAM web-based interface prior to using the system prior to accessing or using the technology.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Director of Probation Services or designee will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Probation Services. All sworn Probation Services personnel will be trained on the Surveillance Technology policy.

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

- Director of Probation Services – 8416
- Senior Supervising Probation Officer - 8415

Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to standard JPD departmental policies, which may include disciplinary action up to and including termination. Every situation is evaluated on a case-by-case basis depending on circumstances surrounding any violations.

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:

Complaints to the Department are accepted in any format, via any means: phone call, verbal to a staff member, email or by written Complaint Form from the SFJPD website. Members of the public can find more information about how to register complaints on the Department's web site: https://sfgov.org/juvprobation/complaints

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

All complaints are directed to the Chief Probation Officer wherein each complaint is assigned a number, and tracked according to AB-953 by date. A receipt letter is sent to each complainant upon delivery of the complaint to the Chief Probation Officer verifying their complaint has been received. The complaint investigation is then assigned by the Chief Probation Officer to staff who to report back directly to the Chief Probation Officer. Once the complaint has been investigated, a follow-up letter shall be sent to the complainant which includes outcomes from the investigation.

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.

Surveillance Impact Report

Sensource Patron Counter System
Public Library

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Sensource Patron Counter System.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is:

The San Francisco Public Library (SFPL) is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

In line with its mission, the Department uses Sensource Patron Counter System to track meaningful operational metrics that show patron entrance/exit traffic throughout our 28 public facilities.

The Department shall use Sensource Patron Counter System only for the following authorized purposes:

- to tally the entry and exit of Library visitors at all 28 public facilities.
- to track usage of meeting rooms, elevators and restrooms for purposes of resource allocation.

There are no additional uses employed by or authorized by the Library. Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is located in the following locations: The110 Sensource devices are installed above entry/exit points at each of the Library's 28 public facilities, including elevator banks and the external doorways of some restrooms and meeting rooms. They are generally affixed to the ceiling above the entranceway.

Surveillance Oversight Review Dates

COIT Review: April 21, 2022
Board of Supervisors Review: TBD

Technology Details

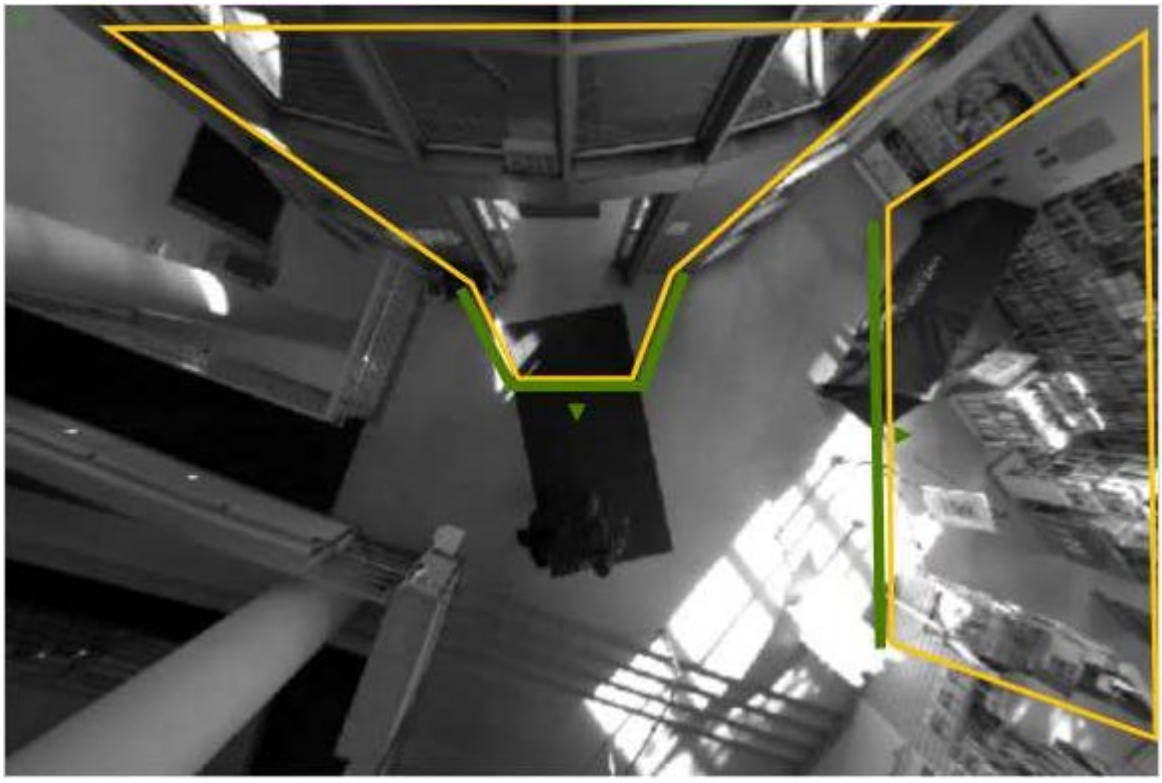
The following is a product description of Sensource Patron Counter System:

SenSource technologies are used by libraries across North America for data-driven decisions. Not only do we offer the most accurate people counting system, it's also expandable to new features such as occupancy monitoring and facemask detection, securing your investment for years to come. Patron traffic data is used to determine total library usage to report for government funding; to optimize staff and scheduled events based on forecasted traffic; and to justify the need for expansion or remodel.

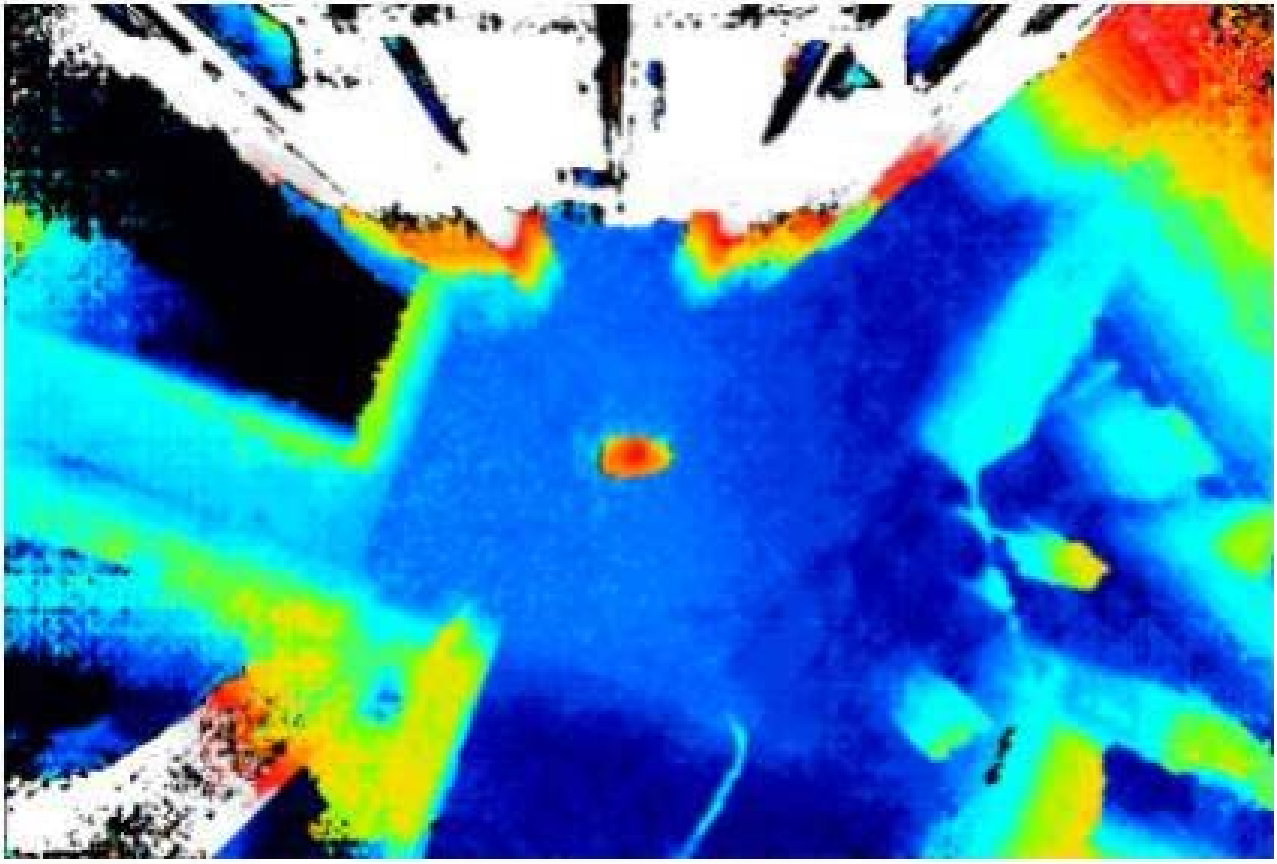
A. How It Works

To function, Sensource Patron Counter System uses a proprietary camera system to tally visitor counts **in real time** at all 28 San Francisco Public Library facilities. **The video images are not recorded or stored.** The aggregate tally data is stored on a cloud-based server and is accessible through web-connected devices.

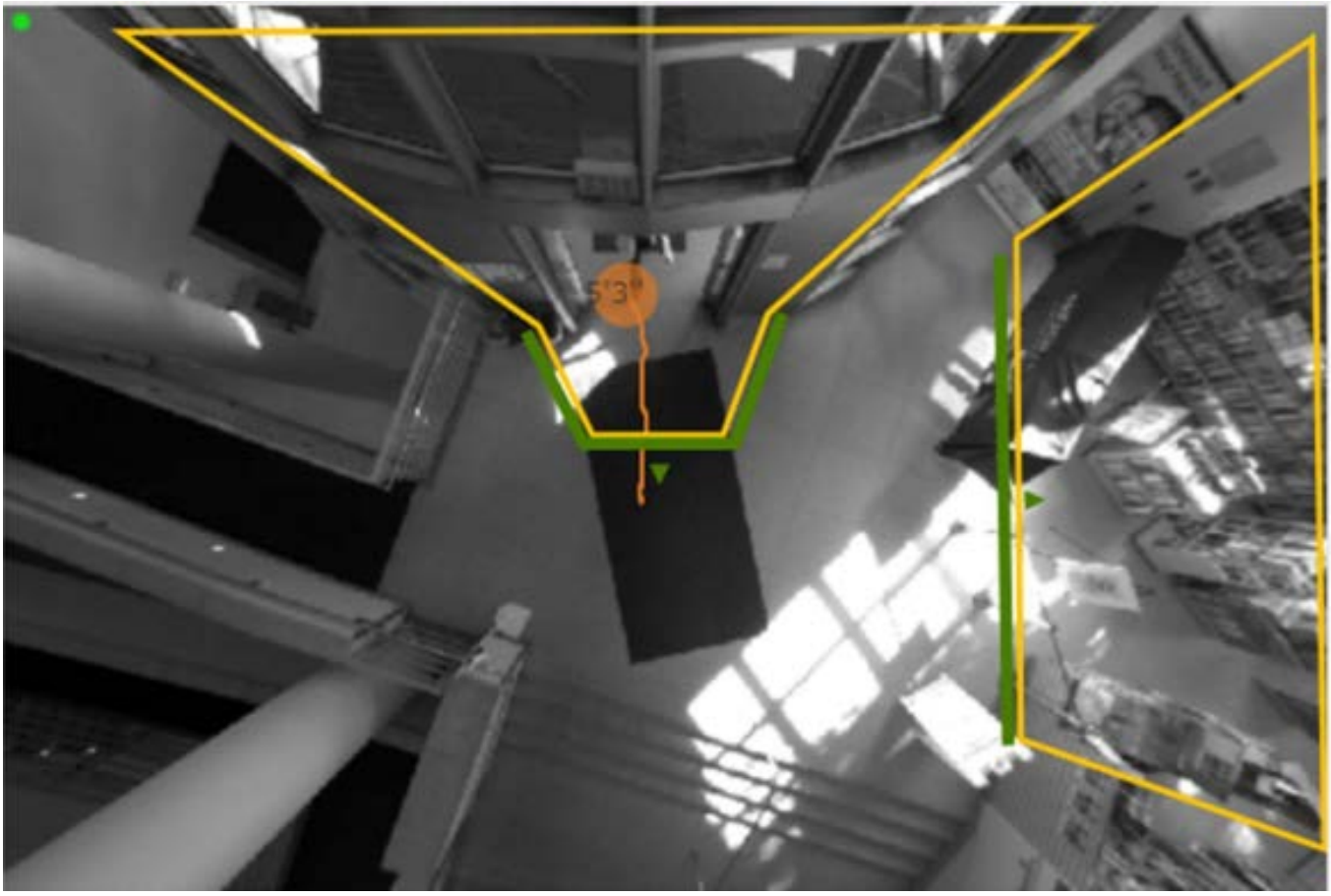
The devices are mounted overhead and produce a low quality black and white image. This is a still-frame image of what the Sensource devices see:



The sensors know their mounted height from the floor and that its individual lenses are 3" apart. It then uses trigonometry to create a Stereo Height map from the 2 images it sees. It then monitors the resulting Stereo height map for anomalies, as in the case of something moving through the scene:



The algorithm analyzes the moving object to see if it fits the known characteristics of a humanoid shape. The red area in the shape of the top of a head. The symmetric orange showing a shoulder shape to the object and then the light green of arms and legs. If it sees these indicators it will consider this to be a trackable object and continue to utilize these height maps to track the object while it is visible to the sensor.



It then tracks the moving object through the scene to see if it crosses a counting line. And then if it meets all of the rules for the count line its count event will be added to the internal storage tally and then the aggregated count data (**not the video images**) is sent to the server in simplified form:

- Line 1, 11:45:00 am, 1-22-22, FW 1, BW 1
- Line 1, 12:00:00 pm, 1-22-22, FW 0, BW 5

All data collected or processed by Sensource Patron Counter System will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by Sensource, Inc. to ensure the Department may continue to use the technology.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of Sensource Patron Counter System has the following benefits for the residents of the City and County of San Francisco:

- X Community Development: The ability to track accurate patron counts by location in real-time is integral to provision of Library services planning with respect to resource allocation (e.g., staffing, planning for programs, ensuring public safety, etc.).
- X Criminal Justice: Library services benefit the residents of the community in numerous ways, including but not limited to education (programming), health (programming), workforce development/jobs (adult programming), community engagement/development (programming), environmental concerns (programming), housing (programming), criminal justice (programming) and public safety (ensuring crowd sizes are appropriate for spaces).
- X Education: See above.
- X Environment: See above.
- X Health: See above.
- X Housing: See above.
- X Jobs: See above.
- X Library Services: See above.
- X Public Safety: See above.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

Though the potential for impact is very low, SFPL limits access to staff responsible for maintaining the devices as well as those validating and collecting aggregate visitor data.

- Technical Safeguards: Access to the Sensource Patron Counters System is password-protected and users are validated for business need on an annual basis.
- Physical Safeguards: SFPL servers are behind two locked doors requiring keycard access. The first level of keycard access is limited to IT staff and high-level individuals in the organization (City Librarian, other department heads, etc.). The second level of keycard access requires both the validated keycard and an individual PIN code. This is limited exclusively to individuals in the IT Division who have a business reason to access servers – primarily the library's DISO (department information security officer) and server team, as well as other IT managers with need to directly access the data center.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Sensource Patron Counter System yields the following business and operations benefits:

- X Financial Savings: Visitor traffic is a core metric within the library industry, reported at the national, state and local levels as a key performance indicator. The Sensource Patron Counter System allows for considerable financial and time savings, as what was previously a manual data collection and analysis process has become automated, allowing for real-time review and data analysis.
- X Improved Data Quality: Data quality has become much more reliable and valid through automation.
- X Staff Safety: Staff safety with respect to planning and managing busy times and crowding with respect to popular programming (e.g., Night of Ideas) is also a befefit to department operations
- X Time Savings: See "Financial Savings".

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): The technology does not require additional FTE; however, it is supported by staff members representing the following classifications:
    - 0.02 FTE - 1822 Administrative Analyst
    - 0.01 FTE - 1823 Senior Data Analyst

- The annual costs are:
    - Total Salary & Fringe: $4,614.71
    - Software: $47,000.00
    - Hardware/ Equipment: $6,500.00
    - Professional Services: 0
    - Training: 0
    - Other: 0

The Department funds its use and maintenance of the surveillance technology through Sxn. 16.109 City Charter - Library Preservation Fund.

COMPARISON TO OTHER JURISDICTIONS

Sensource Patron Counter Systems are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Sensource Patron Counter System
San Francisco Public Library

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 Sensource Patron Counter 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

The San Francisco Public Library ("SFPL", "Library", or "Public Library") is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Sensource Patron Counter System 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 Sensource Patron Counter System, 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 Sensource Patron Counter System technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy. There are no additional uses employed by or authorized by the Library.

Authorized Use(s):

– To tally the entry and exit of Library visitors at all 28 public facilities.
– To track usage of meeting rooms, elevators and restrooms for purposes of resource allocation.

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

Departments 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. 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

Sensource Patron Counter System supports the Department's mission and provides important operational value in the following ways:

The Sensource Patron Counter System allows SFPL to track meaningful operational metrics that show patron entrance/exit traffic throughout our 28 public facilities.

In addition, Sensource Patron Counter System promises to benefit residents in the following ways:

- X Community Development: The ability to track accurate patron counts by location in real-time is integral to provision of Library services planning with respect to resource allocation (e.g., staffing, planning for programs, ensuring public safety related to space capacity, etc.).
- X Criminal Justice: Library services benefit the residents of the community in numerous ways, including but not limited to education (programming), health (programming), workforce development/jobs (adult programming), community engagement/development (programming), environmental concerns (programming), housing (programming), criminal justice (programming) and public safety (ensuring crowd sizes are appropriate for spaces).
- X Education: See above.
- X Environment: See above.
- X Health: See above.
- X Housing: See above.
- X Jobs: See above.
- X Library Services: See above.
- X Public Safety: See above.

Sensource Patron Counter System will benefit the department in the following ways:

- X Financial Savings: Visitor traffic is a core metric within the library industry, reported at the national, state and local levels as a key performance indicator. The Sensource Patron Counter System allows for considerable financial and time savings, as what was previously a manual data collection and analysis process has become automated, allowing for real-time review and data analysis.
- X Improved Data Quality: Data quality has become much more reliable and valid through automation.
- X Staff Safety: Staff safety with respect to planning and managing busy times and crowding with respect to popular programming (e.g., Night of Ideas) is also a benefit to department operations
- X Time Savings: See "Financial Savings".

To achieve its intended purpose, Sensource Patron Counter System (hereinafter referred to as "surveillance technology") uses a proprietary camera system (shown in more detail in the SIR) to tally visitor counts in real time at all 28 San Francisco Public Library facilities. The aggregated tally data (not video images) is stored on a cloud-based server and is accessible through web-connected devices.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- The Patron Counter cameras provide a real-time video stream that shows humanoid forms of people walking through the Sensource viewing area from above, providing visual and location data but SFPL does not retain this data and such real-time viewing is limited to administrator access. SFPL only retains aggregate data showing the total number of persons entering/exiting through a viewable space serviced by the Sensource Patron Counter System. This aggregate data is stored in software on the cloud owned and maintained by Sensource, Inc., and then pulled on to SFPL local servers for review, analysis and reporting. **Video images are not recorded or stored.**
- Sensource data in the real-time stream is "Level 3 – Sensitive" on the City's Data Classification Standard. Aggregate data pulled out of Sensource for review, analysis and reporting is "Level 1 – Public".

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:

- Department identification.
- Patrons are notified that activities in a location may be recorded.

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Only staff designated by the City Librarian and/or Chief Operating Officer and Director of Facilities have access to the Sensource Patron Counter System, which is password-protected and limited to staff responsible for maintaining the devices, as well as those validating and collecting aggregate visitor data.

Data must always be scrubbed of PII prior to public use.

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:

- 0964 City Librarian (1)
- 0953 Chief Operating Officer (1)
- 0952 Deputy Director (2)
- 0932 Manager IV (2)
- 1823 Senior Data Analyst (1)
- 1822 Senior Administrative Assistant (2)
- 1840 Junior Management Assistant (1)
- 1801 Analyst Trainee (1)
- 3618 Library Technical Assistant (2)
- 3630 Librarian I (1)
- 3634 Librarian III (3)

B. Members of the public, including criminal defendants

The Public Library 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

The SFPL Facilities division, under guidance from the Chief Operating Officer, maintains a list of staff with password-protected access to the Sensource Patron Counters System, and reviews/updates that list annually for accuracy and alignment with business needs. Further, the Department of Human Resources Employee Handbook addresses Employee Use of City Resources and City Computers and Data Information Systems. Staff are expected to abide by these guidelines as a condition of employment.

Data Sharing: The Public Library will endeavor to ensure that other agencies or departments that may receive data collected by SFPL 's Sensource People Counter Policy 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.

The Public Library 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)

The Public Library shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Public Library 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 currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following non-PII, Level 1 data with the recipients:

Type	**Recipient**
Monthly and annual aggregate totals of visits by location. Note: Video images streamed in real-time are not recorded, stored, or shared.	Controller's Office. SFPL provides performance measures to CON twice a year that shows monthly and annual visits to SFPL facilities. These data are measured by the Sensource Patron Counter System.

Data sharing occurs at the following frequency:

Twice annually.

B. External Data Sharing

Department shares the following non-PII, Level 1 data with the recipients:

Type	Recipient
Aggregate totals of visitors in text format. Note: Video images streamed in real-time are not recorded, stored, or shared.	California State Library. American Library Association. Public Library Association. Others, upon request. As noted, library visits is a key performance indicator that is shared widely for benchmarking and analysis within the industry. These data are shared in the aggregate, with no PII concerns.

Data sharing occurs at the following frequency:

At least annually, as well as upon request.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

San Francisco Public Library endeavors to comply with all relevent privacy statutes at the federal, state and local levels.

Before data sharing with any recipient, 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 by other means that can accomplish the same purpose.
- X Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.
- X Evaluate what data can be permissibly shared with members of the public should a request be made in accordance with San Francisco's Sunshine Ordinance.
- X Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	Retention Justification
Video images streamed in real-time are not recorded or stored. Aggregate	SFPL keeps aggregate visitor total data indefinitely for historical review and sharing purposes.

visitor count data is stored permanently.	

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.

Data will be stored in the following location:

- Software as a Service Product
- Local Storage

Data Disposal: There is no PII related to the aggregated data retained by the department, so no deidentification or regular disposal is required.

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.

At the very least, 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. 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.

All staff accessing Sensource are given a one-time training on how to use the software and the proper use cases for the aggregate visitor data. This training includes but is not limited to the following components: logging into the system; reviewing available dashboards and how to manipulate filters for their specific needs; how to interpret the dashboards and data within; how to export data; uses for data.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Director of Facilties is responsible for monitoring the Sensource Patron Counter System to ensure that staff do not violate the Library's privacy and compliance policies. .

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

- 0953 - Chief Operating Officer
- 0932 - Director of Facilities

Sanctions for violations of this Policy include the following:

- First Offense: Staff who use the system inappropriately will receive initial counseling on appropriate use of Sensource within the organization.
- Second Offense: Staff will be put on probation for 3 months from using the system.
- Third Offense: Staff will be prohibited from using the system.

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:

Members of the public can register complaints/concerns or submit questions in writing via the Library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's

Office, Main Library, 100 Larkin Street, San Francisco 94102. They can also contact the Library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

Multiple staff monitor SFPL communications portals to ensure that members of the public receive a response within 24 hours.

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.

Surveillance Impact Report

Computer Management System
Public Library

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Today's Business Solutions (TBS) Computer Time and Print Management.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is the following: The San Francisco Public Library system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

In line with its mission, the Department uses Today's Business Solutions (TBS) Computer Time and Print Management to do the following:

- The computer time management portion of the technology is the mode by which the library is able to provide free, equitable access to public computing resources to its patrons.
- The print management solution is a comprehensive document management solution that allows library patrons to print from library computers and their own devices, as well as to create copies, send faxes, scan documents to electronic storage media, etc.
- Both of these functionalities support access to information as well as to services (e.g., government programs and resources, job applications, etc.)

The Department shall use Today's Business Solutions (TBS) Computer Time and Print Management only for the following authorized purposes:

– *The authorized use case for the TBS Computer Time and Print Management tool is to provide time-delimited public access to library computers and allow the public to print, copy, scan and fax documents, as well as track usage of computers and print resources throughout the library's 28 facilities for purposes of resource allocation and management. The five specific components within TBS Computer Time and Print Management are as follows:*
– *MyPC: Manages patron access to library computers and regulates amount of time each patron can use computers*
– *EZ Booking: Allows patrons to manage their reservations in MyPC, schedule public computer use, etc.*

Surveillance Oversight Review Dates
COIT Review: June 16, 2022
Board of Supervisors Review: TBD

– *Papercut/EPrintIt: Manages public print jobs sent from library computers and patrons' personal devices, allowing them to print their documents on library printers* – *Papercut/ePrintIt: Allows select library staff members, in the interest of customer service and support, to retrieve and print jobs submitted to the system by users during the 24-hour period in which documents are retrievable.. This allows staff to print jobs when printers fail, when print jobs do not meet user expectations, to intermediate when users are struggling with technology, etc.*
– *ScanEZ: Allows library patrons to scan, manipulate, manage, print, email, fax and save documents using either the library's flat-bed or document feeder scanners.*
– *Payment Kiosk: Allows patrons to pay for print and copy jobs processed through Papercut/EPrintIt and/or ScanEZ.*

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is installed on each of the library's approximately 710 public access computers and on each of the 38 ScanEZ workstation interfaces.

Technology Details

The following is a product description of Today's Business Solutions (TBS) Computer Time and Print Management:

The TBS print/time, scan, and payment kiosk system consists of five different components that are all integrated into one user-friendly solution.

- MyPC: The TBS time/rules system software, MyPC, allows for library customers to logon to the public use computers with their library card number or guest pass, which also then authenticates the user into the print system, and allows for the user to work on the public use computers for a defined amount of time. MyPC uses a patron's library card number as an identifier for authentication against the Integrated Library System's (ILS) user database to validate that the user is allowed to use library computers.
- EZ Booking: EZ Booking is the simplified user interface that allows patrons to easily access the MyPC system.
- Papercut/EPrintIt: TBS's print system, PaperCut and EPrintIt, consists of direct input of print jobs into the system by users who send print jobs from in-library public use computers as well as remote input by users who send from their personal devices into the mobile print solution. The TBS system funnels output of all print jobs into a unified print queue.
- ScanEZ. The fourth component is the ScanEZ station, which just allows patrons to scan documents and send them to different outputs (print, email, save to device, etc.). These units do not retain any user information or documents.

- Payment Kiosk: Finally, the payment solution consists of TBS payment devices comprised of payment kiosk units equipped with a hold-and-release device, cash handing for coin and bills, as well as a closed-loop, PCI-compliant credit card unit.

All TBS systems are hosted internally on SFPL servers; they do not communicate with the outside world. The only portions of the overall system configuration that reach outside of the library's on-premises data structure are the mobile print system, EPrinttIt, which allows patrons to submit print jobs through a secure web portal, and the credit card payment solution, which utilizes a dedicated, secure cellular connection to process payments.

A. How It Works

To function, Today's Business Solutions (TBS) Computer Time and Print Management allows patrons to use their library card numbers to schedule sessions and log into library public computers, and manages the amount of time they can use the computers. When they log in, the technology uses an API connection to the library's patron database to validate that the person logging in is an authorized user in good standing. The technology also tethers any print jobs they might send from public computers to their log-in credentials (library card number, PIN) for ease of retrieval.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of Today's Business Solutions (TBS) Computer Time and Print Management has the following benefits for the residents of the City and County of San Francisco:

X	Library Services	This technology benefits residents by broadly supporting a wide range of Library Services - It allows patrons to access the internet free of charge, which in turn gives them access to resources that can benefit their education, health, employment, housing situation, and interaction with the criminal justice system. It provides inexpensive access to printing, copying, faxing, and scanning of documents, which also benefits the public in the aforementioned ways. It allows

		staff to be better able to serve the public with more useful tools, as well as to allow the library to provide more meaningful service to its patrons by more efficiently providing service and managing resources.

A. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

Though the potential impact is very low, SFPL limits access to staff responsible for maintaining the systems and collecting aggregate computer use and print data, as well as minimizing data access of those providing direct public service

The Department's technical safeguards are that access to the TBS Computer Time and Print Management system is password protected and users are validated for business need on an ongoing and annual basis. Specific patron computer usage information is automatically purged from the system nightly. The only computer usage data tracked by the Department is anonymized log-in and duration of use information. The library keeps track of the aggregate number of computer users and the amount of computer time they have used. Per the privacy section of its Internet and Computer Use Rules & Policies (see Appendix A), "The Library does not monitor an individual's use of the Internet. Computer search stations are programmed to delete the history of a user's Internet session once the session is ended. The Computer Booking history is deleted every day." The library's Internet Use Policy (see Appendix B) also states, "The Library does not monitor an individual's use of the Internet."

Data associated with specific patron print/copy/fax/scan functions is purged from the system every 24 hours as well.

The Department's physical safeguards are that SFPL servers are behind two locked doors requiring keycard access. The first level of keycard access is limited to IT staff and high-level individuals in the organization (City Librarian, COO, other department heads). The second level of keycard access requires both a validated keycard and individual PIN code. This access is limited exclusively to individuals in the IT Division who have a business reason to access servers -- primarily the library's Department Information Security Officer (DISO), server team, CIO, and IT managers whose work necessitates access to the data center.

B. Fiscal Analysis of Costs and Benefits

The Department's use of Today's Business Solutions (TBS) Computer Time and Print Management yields the following business and operations benefits:

X	Financial Savings	This technology implementation allows the library to eliminate leases on expensive multi-function devices (MFDs) for the public in favor of simple output devices (printers) that couple with the TBS scan

		hardware to increase the range of functionality. By implementing this technology, the library is able to efficiently combine several products (computer time management; print management; public cloud printing solution) into one product and save on costs associated with separate systems
X	Improved Data Quality	The combination of systems eliminates the need for a labor-intensive in-house print management solution and unified computer use and printing in a way that benefits patrons and streamlines IT support. Also, the simple fact of a computer time management system means that front-line public service staff does not have to actively manage or supervise computer use -- a significant staff time savings.
X	Time Savings	Reporting on both computer usage and printing (aggregate number of sessions; number of hours used/day/week/month/year; time of day used; number of pages printed, etc.) is made significantly easier and more meaningful with the unified system and single data access portal.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing):
    - 3634 (1) Librarian III
    - 1095 (1) IT Operations Support Admin V
    - 1093 (1) IT Operations Support Admin III
- The one-time costs are:
    - Total Salary & Fringe: 0
    - Software: 0
    - Hardware/ Equipment: $103,406
    - Professional Services: 0
    - Training: 0
    - Other: 0
- The annual costs are:
    - Total Salary & Fringe: $27,798
    - Software: $525,293
    - Hardware/ Equipment: 0
    - Professional Services: $3,696
    - Training: 0
    - Other: 0

The Department funds its use and maintenance of the surveillance technology through the Library IT Budget and the Library Preservation Fund.

COMPARISON TO OTHER JURISDICTIONS

Today's Business Solutions (TBS) Computer Time and Print Management are currently utilized by other governmental entities for similar purposes.

Appendix A: San Francisco Public Library Internet Use Policy

Internet and Computer Use Rules & Policies

See also: Internet Use Policy

Computer Use Mission Statement

To fulfill its mission of providing free and equal access to information, knowledge, independent learning and the joy of reading to our diverse community, the San Francisco Public Library (SFPL) provides access to the Internet and to personal computers with a variety of software.

Computer Policies

- Internet Disclaimer
- Privacy
- Network Security
- Open Access Policy FAQs (PDF) Chinese| English| Russian| Spanish)
- USA PATRIOT Act and PATRIOT Act FAQs
- Rules and Responsibilities for the Public

Computer Policies

The Internet and online environment consists of information on a wide range of topics provided by millions of individuals and organizations around the world. Not all information found on the Internet is accurate, complete, up-to-date, legal or philosophically acceptable to all individuals. While SFPL can sometimes suggest Internet sites:

Internet Disclaimer

- SFPL does not monitor or control the content of the material accessed through the Internet and cannot be held responsible for its contents. (Internet Use Policy 206, paragraph IV)
- Internet users are responsible for evaluating the accuracy of material found on the Internet
- In accordance with Ch. 22-C.3 of the San Francisco Administrative Code, Ordinance 206-01, SFPL does not employ filtering software
- SFPL does not and cannot assume liability for damages from use of Internet information. (Internet Use Policy 206, paragraph IV)
- SFPL employs antivirus software, but it cannot warrant that its Web site, server, or any other Web site accessed by Internet users is free of viruses or other harmful components.

For further guidance, SFPL collections include Reference and Circulating resources on navigating and evaluating Web sites.

Privacy

SFPL champions the protection of personal privacy. SFPL will keep confidential all such information that it purposefully or inadvertently collects or maintains to the fullest extent permitted by federal state and local law, including the California Public Records Act, the San Francisco Sunshine Ordinance, and the USA PATRIOT Act.

- The Internet is not a secure medium. Email is not necessarily secure against interception.
- The Library does not monitor an individual's use of the Internet. Computer search stations are programmed to delete the history of a user's Internet session once the session is ended. The Computer Booking history is deleted every day.
- Internet computers are provided with privacy screens for your privacy. In accessing various Internet sites, please be conscious of others in your vicinity, particularly children.
- SFPL does not provide information about patrons' library records, use of other SFPL materials, or use of the Internet to law enforcement officials without an appropriate court order. However, law enforcement officers may take action on their own if they observe illegal activity in plain view. Internet users are reminded that illegal use of the Internet is prohibited by State and Federal laws, and by SFPL policy.

For more information on privacy issues and Internet use, please see SFPL's complete Privacy Policy and Internet Use Policy.

Network Security

For Website security and to ensure that service remains available to all library users, SFPL electronically monitors network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage. Anyone using the SFPL Website expressly consents to such monitoring. Except for the above purposes, or if required by law, no other attempts are made to identify library users or their Web activity.

USA PATRIOT Act

(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) Sections 214-216 of this Act gives law enforcement agencies expanded authority to obtain library records, monitor electronic communications and prohibits libraries and librarians from informing library users of monitoring or information requests. The Library Commission and the San Francisco Board of Supervisors have formally opposed the Act, including Sections 214-216, in two separate resolutions. [Resolutions #136-04 and #053-03]. On March 2, 2004, San Francisco voters codified the City's resistance to the federal USA PATRIOT Act with their approval of Proposition E. The charter amendment

requires that any request for library, health or other personal records be routed through the Board of Supervisors instead of through City department heads. The supervisors will then decide whether the request is constitutional and whether to respond to it. For more information on the USA PATRIOT Act, please see SFPL's Privacy Policy and USA PATRIOT Act Resolution.

Rules and Responsibilities for the Public

Use of SFPL's equipment for the transmission, dissemination, and/or duplication of information must comply with federal and state laws. SFPL expects all users to comply with such laws, including but not limited to those related to copyright, computer hacking, and child pornography. Computer users will also refrain from any activity that unreasonably interferes with SFPL patron/staff comfort, safety, use or quiet and peaceful enjoyment of the library, including but not limited to:

- Harassing or threatening Library users or staff.
- Making any loud or unreasonable noise, or other disturbance, including disruptive use of personal communications or entertainment devices.
- Vandalizing or abusing computer equipment, including removing privacy screens, tampering with equipment or software.
- Using the library card number of another person, including a relative, to access the computer system.
- Hacking into the computer systems.
- Manipulating SFPL computer systems to override established time limits.
- Refusing to leave a computer after being suspended from computers, or continuing to create a disturbance while using SFPL equipment.
- Viewing of any illegal, offensive, or harmful matter1, including but not limited to pornography within any area designated for children or teens.

Additionally, SFPL has the following expectations of computer users:

- Comply with a Library staff member reasonable request to refrain from or change a disruptive behavior.
- Comply with Internet etiquette as stated in Guidelines for Library Use and in this document.
- Refrain from harming SFPL computers or systems through the use of viruses or other malicious acts.
- Refrain from installing or copying software to SFPL computers.

Persons who violate these Rules and Responsibilities may receive a warning from SFPL staff and/or an opportunity to cease the violation or leave the Library. Illegal activity, as well as any willful or repeated violations of these Rules and Responsibilities or other posted SFPL regulations, may result in removal from the facility and/or suspension of SFPL privileges. Violation of law may result in arrest and prosecution. In addition, where authorized by Federal, State or local law, violations of these Rules and Responsibilities may also result in arrest.

For more information on SFPL Rules and Responsibilities, please see Guidelines for Library Use and Internet Use Policy. For more information on the Digital Millennium Copyright Act, visit the United States Copyright Office Web site (http://lcweb.loc.gov/copyright/).

Children and Teens

As with other library materials, restricting a child or teen's access to the Internet is the responsibility of the parent or legal guardian. It is recommended that parents or guardians discuss safe Internet practices with their children. For more information, please see SFPL's Internet Use Policy and the SFPL Kids webpage section: Going Online.

Computer Etiquette

- While waiting for computer availability, please respect the privacy of the current user.
- Please do not prevent others from claiming computer reservations or turns at Internet computers either verbally or physically (i.e., sitting at the computer without being logged in).
- Any question or conflict about computer reservations should be referred to Library staff on duty. You may be asked to submit your library card number to resolve the issue. Our goal is to provide access to all who wish to use the public computers, and we will do everything we can to resolve the situation to everyone's satisfaction.
- Please keep your belongings with you at all times. The Library is not responsible for loss or damage to personal belongings. Unattended belongings may be picked up by Library staff and removed either to the nearest Reference Desk, or to the Security Office.
- Please keep all conversation, including cell phone use, at a low volume.
- Please move to designated areas to talk on your cell phone.
- Please be courteous to other users by following the Guidelines for Library Use.

Number of Persons Per Computer

Librarians may, at their discretion, limit use of computer terminals to one or two patrons as needed to ensure comfort, safety, use, or quiet and peaceful enjoyment of the Library for all Library users and staff. Patrons may be allowed to work collaboratively, if their behavior causes no disruption.

Disclaimer for Assistance with Patron Mobile Devices (PDF). English | Chinese | Spanish

Appendix B: San Francisco Public Library Internet Use Policy

Internet Use Policy

See also: Privacy Policy Policy #206: Adopted December 1998. To fulfill its mission of providing free and equal access to information, knowledge, independent learning and the joy of reading to our diverse community, the San Francisco Public Library provides access to the Internet.

The Internet

The Internet consists of information on a wide range of topics provided by millions of individuals and organizations around the world.

Disclaimer

Links to Internet sites can be found on the home web pages designed by the staff of the San Francisco Public Library. The Library follows its materials selection guidelines in linking other web sites to its home pages. Beyond this, the Library has not participated in the development of these other sites and does not exert any editorial or other control over these sites. Any link from the Library's web site to another web site is not an endorsement from the Library. The Library does not warrant that its web site, the server that makes it available, or any links from its site to other web sites are free of viruses or other harmful components.

User Responsibility

The Library does not monitor or control the content of the material accessed through the Internet and cannot be held responsible for its contents. Not all information found on the Internet is accurate, complete, up-to-date, legal or philosophically acceptable to all individuals. The Library assumes no responsibility and shall have no liability for any direct, indirect or consequential damages arising from the use of information found on the Internet, or any communications sent through the Library's Internet terminals. The Library does not monitor an individual's use of the Internet; nor does the Library employ filtering software.

Access and Usage

The Library does not provide email accounts to users; however, users with existing email accounts may access their accounts through the Library's Internet terminals. The Library assumes no responsibility and shall have no liability for any claims or damages which result from the provision of such access to users.

As with other library materials, restriction of a child's access to the Internet is the responsibility of the parent or legal guardian.

Use of the Library's terminals for the transmission, dissemination, and/or duplication of information is regulated under various state and federal laws. The Library expects all users to comply with such laws.

The Library has developed Computer Help & Rules pages. In addition, the Library Commission has adopted "Guidelines for Library Use" for the Library (Policy #SFPL-201 rev. 8/07). Any users of the Library's Internet terminals must follow these Rules and the Guidelines for Library Use.

Approved by Library Commission: 12/98

Surveillance Technology Policy

Computer Management System
Public Library

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 Today's Business Solutions (TBS) Computer Time and Print Management 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:

The San Francisco Public Library system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Today's Business Solutions (TBS) Computer Time and Print Management will be used to support this mission, by describing the 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 Today's Business Solutions (TBS) Computer Time and Print Management, 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 Today's Business Solutions (TBS) Computer Time and Print Management technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– *The authorized use case for the TBS Computer Time and Print Management tool is to provide time-delimited public access to library computers and allow the public to print, copy, scan and fax documents, as well as track usage of computers and print resources throughout the library's 28 facilities for purposes of resource allocation and management.The five specific components within TBS Computer Time and Print Management are as follows:*
– *MyPC: Manages patron access to library computers and regulates amount of time each patron can use computers*
– *EZ Booking: Allows patrons to manage their reservations in MyPC, schedule public computer use, etc.*

COIT Policy Dates
COIT Review: June 16, 2022
BOS Approval: TBD

– *Papercut/EPrintIt: Manages public print jobs sent from library computers and patrons' personal devices, allowing them to print their documents on library printers* – *Papercut/ePrintIt: Allows select library staff members, in the interest of customer service and support, to retrieve and print jobs submitted to the system by users during the 24-hour period in which documents are retrievable. This allows staff to print jobs when printers fail, when print jobs do not meet user expectations, to intermediate when users are struggling with technology, etc.*
– *ScanEZ: Allows library patrons to scan, manipulate, manage, print, email, fax and save documents using either the library's flat-bed or document feeder scanners.*
– *Payment Kiosk: Allows patrons to pay for print and copy jobs processed through Papercut/EPrintIt and/or ScanEZ.*

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

Departments 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. 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

Today's Business Solutions (TBS) Computer Time and Print Management adds to the Department's mission and provides important operational value in the following ways:

The computer time management portion of the technology is the mode by which the library is able to provide free, equitable access to public computing resources to its patrons. The print management solution is a comprehensive document management solution that allows library patrons to print from library computers and their own devices, as well as to create copies, send faxes, scan documents to electronic storage media, etc. Both of these functionalities support access to information as well as to services (e.g., government programs and resources, job applications, etc.).

In addition, Today's Business Solutions (TBS) Computer Time and Print Management promises to benefit residents in the following ways:

X	Library Services	This technology benefits residents by broadly supporting a wide range of Library Services - It allows patrons to access the internet free of charge, which in turn gives them access to resources that can benefit their education, health, employment, housing situation, and interaction with the criminal justice system. It provides inexpensive access to printing, copying, faxing, and scanning of documents, which also benefits the public in the aforementioned ways. It allows staff to be better able to serve the public with more useful tools, as

		well as to allow the library to provide more meaningful service to its patrons by more efficiently providing service and managing resources

Today's Business Solutions (TBS) Computer Time and Print Management will benefit the department in the following ways:

X	Financial Savings	This technology implementation allows the library to eliminate leases on expensive multi-function devices (MFDs) for the public in favor of simple output devices (printers) that couple with the TBS scan hardware to increase the range of functionality. By implementing this technology, the library is able to efficiently combine several products (computer time management; print management; public cloud printing solution) into one product and save on costs associated with separate systems
X	Improved Data Quality	The combination of systems eliminated the need for a labor-intensive in-house print management solution and unified computer use and printing in a way that benefits patrons and streamlines IT support. Also, the simple fact of a computer time management system means that front-line public service staff does not have to actively manage or supervise computer use -- a significant staff time savings.
X	Time Savings	Reporting on both computer usage and printing (aggregate number of sessions; number of hours used/day/week/month/year; time of day used; number of pages printed, etc.) is made significantly easier and more meaningful with the unified system and single data access portal.

To achieve its intended purpose, Today's Business Solutions (TBS) Computer Time and Print Management (hereinafter referred to as “surveillance technology”) allows patrons to use their library card numbers to schedule sessions and log into library public computers, and manages the amount of time they can use the computers. When they log in, the technology uses an API connection to the library's patron database to validate that the person logging in is an authorized user in good standing. The technology also tethers any print jobs they might send from public computers to their log-in credentials (library card number, PIN) for ease of retrieval.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Scanned Images	XML, PDF, HTM, Plain Text, TIFF, JPEG, PNG, GIF, CSV	Level 1-3

- Print/copy/scan: most level 1 - Examples of patron prints/scans/etc. listed previously (e.g., tax returns, medical records) could be classified as Level 3, depending on content.

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:

- Description of the authorized use
- Information on the surveillance technology

Patrons must accept the library's Rules for public computer use each time they log into the library's computers.

Both the Computer Use Rules and Responsibilities for the Public, which users accept when logging into library computers, and the ePrintIt portal for web printing, inform users that documents submitted to the TBS system may be retrieved for up to 24 hours, after which time they are purged from the system.

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- All public service staff have access to the computer reservation and print modules of the system. Only staff designated by the City Librarian and/or Chief Operating Officer and the Chief Information Officer have access to the reporting capabilities of the system where aggregate data is stored.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- 0964 City Librarian (1)
- 0953 Chief Operating Officer (1)
- 0952 Chief Information Officer (1)
- 3634 Librarian III/Digital Strategist (1)
- 1095 IT Operations Support Admin V / Desktop Support (1)
- 1094 IT Operations Support Admin IV (1)
- 1093 IT Operations Support Admin III (5)
- 1823 Senior Administrative Analyst (1)

B. Members of the public, including criminal defendants

The Public Library 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

The Department will not produce documents for a Sunshine Ordinance or California Public Records Act request if such request is directed at obtaining private patron documents sent for printing, scanning, or copying by library users; these documents are the private personal documents of the user; they are not related to library's normal course of business, nor are they considered city records.

The Department will follow its existing Privacy Policy with respect to subpoenas, USA PATRIOT Act requests, administrative orders and any such legal request by a judicial body of law.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

The SFPL Information Technology Division, under guidance from the Chief Operating Officer, maintains a list of staff with password-protected access to the aggregate data available in the TBS Computer Time and Print Management system, and reviews and updates that list annually for accuracy and alignment with business needs. Further, the Department of Human Resources Employee Handbook addresses Employee Use of City Resources and city Computers and Data Information Systems. Staff are expected to abide by these guidelines as a condition of employment.

Data Sharing: The Public Library Department will endeavor to ensure that other agencies or departments that may receive data collected by The Public Library's Today's Business Solutions (TBS) Computer Time and Print Management Policy 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.

The Public Library 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)

The Public Library Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Public Library 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 currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Type	Recipient
Monthly and annual aggregate totals of public computer use by location.	Controller's Office: SFPL provides performance measures to CON twice a year that show monthly and annual computer use. These data are measured by the TBS Computer Time and Print Management system.

Data sharing occurs at the following frequency:

- Twice annually.

B. External Data Sharing

Department shares the following data with the recipients:

Type	Recipient
Monthly and annual aggregate totals of public computer use and print volumes by location in text format.	California Library Association, American Library Association, Public Library Association, Urban Library Council, and others upon request in accordance with California Public Records Act (CPRA) and San Francisco Sunshine Ordinance.

Data sharing occurs at the following frequency:

- Annually; upon request.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

- San Francisco Public Library endeavors to comply with all relevant privacy statutes at the federal, state, and local levels.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	Retention Justification
Permanent records.	SFPL public computer use and print volume data is retained indefinitely for historical purposes.

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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- n/a

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

X Local Storage

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- N/A as data is kept permanently

Processes and Applications:

- There is no PII related to the aggregated data so no deidentification is required.

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.

At the very least, 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. 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.

Staff accessing TBS Computer Time and Print Management are given a one-time training on how to use the software and proper use cases for accessing aggregate user data. This training includes but is not limited to: logging into the system; reviewing available dashboards; reviewing available report types; how to interpret data in the system; how to export data; uses for data.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Chief Information Officer (CIO) is responsible for monitoring the TBS Computer Time and Print Management system to ensure staff do not violate the library's privacy and compliance policies.

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

- 0953 - Chief Operating Officer
- 0952 - Chief Information Officer

Sanctions for violations of this Policy include the following:

- First Offense: Staff who use the system inappropriately will receive initial counseling on appropriate use of TBS Computer Time and Print Management within the system.
- Second Offense: Staff will be put on probation from using the system for 3 months.
- Third Offense: Staff will be prohibited from using the system.

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:

Complaints or concerns can be submitted to the Department by:

> Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library, 100 Larkin St., San Francisco, 94102. They also can contact the library by phone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- Multiple staff monitor SFPL communications portals to ensure the members of the public receive a response within 24 hours.

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.

Surveillance Impact Report

Social Media Monitoring Platform, such as Hootsuite
Public Library

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Social Media Monitoring Platform, such as Hootsuite

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is:

The San Francisco Public Library system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

In line with its mission, the Department uses Social Media Monitoring Platform, such as Hootsuite to enable SFPL to plan, coordinate and schedule its social media postings, which inform the public about the abundance of free programs and resources the library offers. For example, the Library hosted approximately 18,000 public programs a year prior to the pandemic.

The Department shall use Social Media Monitoring Platform, such as Hootsuite only for the following authorized purposes:

- Plan and execute more effective and strategic campaigns across social media platforms.
- Schedule multiple social media posts in advance.
- Create and monitor multiple streams of content across various platforms.
- Maintain active social media presence that is automated, specifically on weekends when staff is off.
- Ensure consistency of messaging across all social media platforms.
- Track post performance and analyze trends to improve content and strategy.
- Create reports.

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is located in the cloud. Hootsuite is a cloud-based software on which SFPL staff will use on CCSF computers and devices.

Surveillance Oversight Review Dates
COIT Review: October 21, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description of Social Media Monitoring Platform, such as Hootsuite:

Hootsuite Media Inc. provides social web marketing services. The Company offers social media dashboards that allow updates to social networks through web, desktop, and mobile platforms and track campaign results and industry trends.

We believe in the power of human connection. We created Hootsuite to help people connect on social media and do amazing things together. We connect people with the communities they live in. The teams they work with. The brands they love. The customers who believe in them. And the leaders and visionaries who show them the way forward.

Whether you're managing a small team or making a bold leap forward to completely transform your social enterprise, Hootsuite is here to help you unlock the power of human connection and make great things happen.

We help organizations build enduring customer relationships at scale. Social media is the center of your customers' online life. It's where they discover products, consume media, and connect with like-minded people. But connecting with customers is just the beginning. Social is an incredibly powerful platform to build strong internal cultures, uncover emotionally rich consumer insights, and unify the customer experience across channels and departments. With our unparalleled expertise, open ecosystem, and customer insights at scale, Hootsuite is uniquely positioned to guide your organization to social success.

A. How It Works

To function, Social Media Monitoring Platform, such as Hootsuite, is a social network manager that allows users to create custom views of all connected social networks. HootSuite can be used to post to multiple social media accounts, manage social media messaging, and coordinate the organization's social media marketing. The platform aggregates social media feeds so that content and trends can be viewed holistically.

All data collected or processed by Social Media Monitoring Platform, such as Hootsuite will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by Hootsuite to ensure the Department may continue to use the technology

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of by Social Media Monitoring Platform, such as Hootsuite has the following benefits for the residents of the City and County of San Francisco:

- **Information**: Hootsuite enables the Library to broadcast information about vital resources for the community such as free job, business and finance support; early literacy programs, including one-on-one tutoring; ESL courses; technology classes and access to other robust educational and research databases.
- **Education**: Residents indirectly benefit from SFPL using Hootsuite because it can better target social media outreach to raise visibility of City and Library services, which include free services like Career Online High School, digital, financial and career literacy workshops, early literacy programs such as storytimes and one-on-one tutoring.
- **Community Development**: Residents indirectly benefit from SFPL using Hootsuite because it can better target social media outreach to raise visibility of City and Library services. Additionally, our neighborhood branches provide a robust system of community hubs. Connecting neighborhood residents through public programming helps strengthen our communities and contributes to the City's resiliancy. For those who do not access traditional media, social media can be a critical tool to connect people to information and then to each other through participation in the Library's programs.
- **Public Safety:** Occasionally, library locations serve as Weather Relief Centers. Social media is one vehicle whereby we spread the word about these essential resources. The Library's social media also supports the larger citywide public safety messaging as evidenced during the pandemic year where the Library shared out key messages related to COVID and vaccine access. The Library also relies on social media to inform the public on the rare occasion when a location must shut down due to a power outage, emergency evacuation and other public safety events.
- **Jobs:** The Library promotes employment opportunities via social media as well as its free resources and programs that help and support people in their job searches.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

Though the potential for impact is very low, SFPL will limit access to staff in the department's communications division.

Prior to granting account credentials the communications director will counsel staff on appropriate and inappropriate use as well as provide access to departmental social media guidelines. Periodic reminders will be sent via email.

The San Francisco Public Library strives to mitigate all potential civil rights impacts through responsible technology and data use policies and procedures, and intends to use social media monitoring software exclusively for aforementioned authorized use cases. All other uses are prohibited.

Through HootSuite, SFPL only has access to posts that have been published by the social media users. Public posts include timelines and posts from public accounts. By contrast, SFPL does not have access to private direct messaging, or messages between private accounts that do not belong to SFPL, or payments. The Department will not utilize geographic tags added by users to postings or commenter demographics to track or intercept residents, nor will the Department access such posts with the intention to maliciously surveil, track or monitor its residents.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Social Media Monitoring Platform, such as Hootsuite yields the following business and operations benefits:

- **Financial savings**: Staff time to manually input social media posts into individual social media posts on days that fall outside the standard 40-hour work week (weekends) would likely require approximately 8 hours of overtime per week (32 hours per month).
- **Time savings**: Staff time to manually input social media posts into individual social media platforms represents a savings of 15 hours a week (between at least 3 staff) or 60 hours per month.
- **Improved Data Quality**: Currently SPFL must mine social media data on engagement via each platform, which is laborious and inefficient. Hootsuite will allow data to be mined and analyzed in a much more efficient and effective manner (often in real-time).

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): The technology <u>does not require additional</u> FTE; however, it will be supported by a cohort of staff members representing the following classifications.
    - 1x - 0952 - Deputy Director II
    - 1x - 9251 - Director of Communications
    - 1x - 1314 - Public Information Officer
    - 1x - 5330 - Graphics Supervisor
    - 2x - 5322 - Graphics Artist
    - 1x - 3610 - Library Assistant
    - 10x - 3632 - Librarian Manager
- The annual costs are:
    - Total Salary & Fringe: $150,491
    - Software: $7,200
    - Hardware/ Equipment: 0
    - Professional Services: 0
    - Training: Included in annual licensing fee.
    - Other: 0

The Department funds its use and maintenance of the surveillance technology through Sxn. 16.109 City Charter - Library Preservation Fund.

COMPARISON TO OTHER JURISDICTIONS

Social Media Monitoring Platform, such as Hootsuite are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Social Media Monitoring Software
San Francisco Public Library

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 Social Media Monitoring Software 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 San Francisco Public Library ("SFPL", "Library", or "Public Library") system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which Social Media Monitoring Software will be used to support this mission, by describing the 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 Social Media Monitoring Software, such as Hootsuite, 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 Social Media Monitoring Software technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Plan and execute more effective and strategic campaigns across social media platforms.
- Schedule multiple social media posts in advance.
- Create and monitor multiple streams of content across various platforms.
- Maintain active social media presence that is automated, specifically on weekends when staff is off.
- Ensure consistency of messaging across all social media platforms.
- Track post performance and analyze trends to improve content and strategy.
- Create reports.

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

Departments 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. 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

Social Media Monitoring Software supports the Department's mission and provides important operational value in the following ways:

Social Media Monitoring Software enables SFPL to plan, coordinate and schedule its social media postings, which inform the public about the abundance of free programs and resources the library offers. For example, the Library hosted approximately 18,000 public programs a year prior to the pandemic.

In addition, Social Media Monitoring Software promises to benefit residents in the following ways:

- **Information:** Social Media Monitoring Software enables the Library to broadcast information about vital resources for the community such as free job, business and finance support; early literacy programs, including one-on-one tutoring; ESL courses; technology classes and access to other robust educational and research databases.
- **Education:** Residents indirectly benefit from SFPL using Social Media Monitoring Software because it can better target social media outreach to raise visibility of City and Library services, which include free services like Career Online High School, digital, financial and career literacy workshops, early literacy programs such as story times and one-on-one tutoring.
- **Community Development:** Residents indirectly benefit from SFPL using Social Media Monitoring Software because it can better target social media outreach to raise visibility of City and Library services. Additionally, our neighborhood branches provide a robust system of community hubs. Connecting neighborhood residents through public programming helps strengthen our communities and contributes to the City's resiliency. For those who do not access traditional media, social media can be a critical tool to connect people to information and then to each other through participation in the Library's programs.
- **Public Safety:** Occasionally, library locations serve as Weather Relief Centers. Social media is one vehicle whereby we spread the word about these essential resources. The Library's social media also supports the larger citywide public safety messaging as evidenced during the pandemic year where the Library shared out key messages related to COVID and vaccine access. The Library also relies on social media to inform the public on the rare occasion when a location must shut down due to a power outage, emergency evacuation and other public safety events.
- **Jobs**: The Library promotes employment opportunities via social media as well as its free resources and programs that help and support people in their job searches.

Social Media Monitoring Software will benefit the department in the following ways:

- **Financial Savings:** Staff time to manually input social media posts into individual social media posts on days that fall outside the standard 40-hour work week (weekends) would likely require approximately 8 hours of overtime per week (32 hours per month).
- **Time Savings**: Staff time to manually input social media posts into individual social media platforms represents a savings of 15 hours a week (between at least 3 staff) or 60 hours per month.
- **Improved Data Quality**: Currently SPFL must mine social media data on engagement via each platform, which is laborious and inefficient. Social Media Monitoring Software will allow data to be mined and analyzed in a much more efficient and effective manner (often in real-time).

To achieve its intended purpose, Social Media Monitoring Software, hereinafter referred to as "surveillance technology"), is a social network manager that allows users to create custom views of all connected social networks. Social Media Monitoring Software can be used to post to multiple social media accounts, manage social media messaging, and coordinate the organization's social media marketing. The platform aggregates social media feeds so that content and trends can be viewed holistically.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- **Classified Data Types**: Social media handles and profiles, personal information (name, date of birth, age, and marital and employment status if included in social media profile); individual and group characteristics and biometric information such as facial recognition, in so far that it is captured by the social media platform, e.g., Facebook and Instagram.
- **Data Formats**: HTML, JPG, PNG, GIF, MOV, MP3, MP4.
- **Security Classification**: Level 1: Name, Social Media Handle, Social profile. Level 2 (Internal Use): Correspondence sent and received through Social Media Software.

Social Media Monitoring Software aggregates data which has already been made public on social media platforms.

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Onboarding and training, including a written social media guidelines document, to advise employees of appropriate and prohibited use.

Data must always be scrubbed of PII prior to public use.

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:

- 0952 - Deputy Director II (1)
- 9251 - Director of Communications (1)
- 1314 - Public Information Officer (1)
- 5330 - Graphics Supervisor (1)
- 5322 - Graphics Artist (2)
- 3610 - Library Assistant (1)
- 3632 - Librarian Manager (10)

B. Members of the public, including criminal defendants

The Public Library 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

The Department of Human Resources Employee Handbook Addresses Employee Use of City Resources and City Computers and Data Information Systems. Additionally, the Department's account on the Social Media Monitoring Software platform is only accessible through user logins created by account administrators within the Department.

Data Sharing: The Public Library will endeavor to ensure that other agencies or departments that may receive data collected by the Public Library's Social Media Monitoring Software 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.

The Public Library 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)

The Public Library shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Public Library 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 currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing

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

Before data sharing with any recipient, the Department will use the following procedure to ensure appropriate data protections are in place:

- Confirm the purposes of the data sharing align with the department's mission.
- Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluate what data can be permissibly shared with members of the public should a request be made in accordance with San Francisco's Sunshine Ordinance.
- Ensured shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period:	Retention Justification:
• General/Administrative: Correspondence, miscellaneous - 2 years • General/Administrative: Statistical - 5 years	The retention period is tied to the SFPL Records Retention and Destruction Policy

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.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

Social Media Monitoring Software contractors, such as Hootsuite, shall store the data in their own cloud storage.

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- Reports generated typically download to a folder of temporary files, sometimes called "downloads" on individual devices. These folders are typically deleted by the user on a regular basis.

Processes and Applications:

- Deleting the report removes all data from the local machine or network.

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.

At the very least, 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. 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.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Director of Communications and Public Information Officer will be responsible for monitoring the platform to ensure that staff do not violate the Library's social media policies.

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

- 9251 - Director of Communications
- 1314 - Public Information Officer

Sanctions for violations of this Policy include the following:

- First Offense: Staff who use the platform inappropriately will receive initial counseling on appropriate use of social media within the organization. The Public Affairs team will also send periodic reminders to staff on best practices regarding appropriate use.
- Second Offense: Staff will be put on probation for 3 months from using the platform.
- Third Offense: Staff will be prohibited from using the platform.

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:

Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library, 100 Larkin Street, San Francisco 94102. They can also contact the library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

Members of the public can also contact the Public Affairs team at publicaffairs@sfpl.org.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

Multiple staff monitor SFPL communications portals to ensure that members of the public receive a response within 24 hours.

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.

Surveillance Impact Report

Department of Elections
Cameras

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The mission of the San Francisco Department of Elections is to provide access to election-related services and voting and to conduct elections that are free, fair, and functional.

In line with its mission, the Department shall use cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring of voting center lines.
2. Live monitoring of Department staff during elections operations.
3. Recording of video and images of Department staff during elections operations.
4. Reviewing camera footage of Department staff in the event of an incident.
5. Sharing camera footage of Department staff with the public to promote transparency into elections operations.

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

Further, processing of personal data revealing 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.

Department technology may be deployed in the following locations, based on use case:

1. Department of Elections in City Hall
2. Department's Warehouse at Pier 31

Surveillance Oversight Review Dates

COIT Review: November 21, 2021
Board of Supervisors Review: TBD

Technology Details

The following is product description:

The Nest Cam Security Camera lets you keep an eye on what matters most to you, even when you're far from home. Take advantage of 24/7 live video streaming to your mobile device or tablet. Get alerts if something happens and watch footage live in 1080p HD.

A. How It Works

To function, streaming cameras capture video at Department of Elections office in City Hall and Warehouse locations. Stream from the City Hall Voting Center is private and is monitored only from inside the Elections office. Streams of ballot processing are streamed publicly on the internet and can be found on the Department's website. Video from streams is stored for 10 days prior to automatic deletion.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of security cameras has the following benefits for the residents of the City and County of San Francisco:

X	Education	Allows the public to watch and learn about the election process in San Francisco.
☐	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
☐	Environment	
☐	Criminal Justice	
☐	Jobs	

☐	Housing	
X	Other	Transparency is a key component of free, fair, and functional elections. To that end, the Department of Elections welcomes members of the public to observe its operations and offer feedback.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

Administrative Safeguards: Recordings can only be accessed by 1092-1095 IS Administrator Series, 1840-1844 Management Assistant series, 1115 Director, 0951-0955 Deputy Director series. Internal streams of voting line are not posted publicly.

Technical Safeguards: Access to recordings is password protected. Recordings are automatically deleted from Google servers after 10 days.

Physical Safeguards: Cameras are located only at secured Department of Elections offices at City Hall and Pier 31.

The Department of Elections strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures, and intends to use Streaming Cameras and their associated data exclusively for aforementioned authorized use cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

Streaming Cameras are used to monitor line of voters to determine if additional personnel are needed at the City Hall Voting Center to ensure efficient service. Live streams of ballot processing activities provide the public with transparent and accessible opportunities to observe election processes.

C. Fiscal Analysis of Costs and Benefits

The Department's use of surveillance cameras yields the following business and operations benefits:

Benefit		**Description**
X	Financial Savings	Streaming cameras allow us to provide election observation activities while minimizing deployment of personnel to staff each observation area.
X	Time Savings	Streaming cameras enable monitoring of election processes happening in different areas of the city at the same time from a central location.
X	Staff Safety	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	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.

The total fiscal cost, including initial purchase, personnel and other ongoing costs is Number of FTE (new & existing)	2 existing employees, Total expected staff hours (all): 10 hrs/election *8 hrs x 1 election x $61/hr:* ***$488/election*** *2 hrs x 1 election x $51/hr:* ***$102/election*** ***Total: $590/election***	
Classification	IS Admin (1092) & Elections Clerk (1403)	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment		21 cameras x $200: **$4,200**/one-time cost
Professional Services		
Training		
Other	Subscription plan for 10 day recording retention: **$2,100**	
Total Cost	***$2,690/yr (1 election), $3,280/yr (2 elections).***	***$4,200***
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR		

The Department funds its use and maintenance of the surveillance technology through

Annual Operating Budget.

COMPARISON TO OTHER JURISDICTIONS

The Nest Cam Security Cameras are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Mapped Crime Statistics

The general location(s) it may be deployed and crime statistics for any location(s).

Surveillance Technology Policy

Security Cameras
Department of Elections

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 Department's 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

The Surveillance Technology Policy ("Policy") defines the manner in which the 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 Camera Systems, 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 Cameras to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring of voting center lines.
2. Live monitoring of Department staff during elections operations.
3. Recording of video and images of Department staff during elections operations.
4. Reviewing camera footage of Department staff in the event of an incident.
5. Sharing camera footage of Department staff with the public to promote transparency into elections operations.

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

Departments may use information collected from security cameras 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.

Surveillance Oversight Review Dates
COIT Review: November 21, 2021
Board of Supervisors Review: Upcoming

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras promise to help with:

X	Education	Allows the public to watch and learn about the election process in San Francisco.
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Transparency is a key component of free, fair, and functional elections. To that end, the Department of Elections welcomes members of the public to observe its operations and offer feedback.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Streaming cameras allow us to provide election observation activities while minimizing deployment of personnel to staff each observation area.
X	Time Savings	Streaming cameras enable monitoring of election processes happening in different areas of the city at the same time from a central location.
X	Staff Safety	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	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	Service Levels	Cameras will enhance transparency of elections operations to the public.

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 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 intended 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
- X Description of the authorized use
- Type of data collected
- Will persons be individually identified
- Data retention
- X Department identification
- X Contact information

Access:	Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses. Access to live views are available to the public via a live-stream video feed, for the duration of the election activities which include voting and vote tallying. Live video footage is made available to the public to provide transparency surrounding city and county elections. Recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident and is automatically deleted 10 days after the recording is made. 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. - 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 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 their own 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. Because this footage is streamed live

to the public, it is possible that viewers of the footage will retain, share, or and use the footage in ways that do not comply with this policy.

Each department that believes another agency or department receives or may receive data collected from its use of 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 data will be shared 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 Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, 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:

- On request following an incident.

B. External Data Sharing:

- Other local law enforcement agencies

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 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:

- Camera data will be stored for a minimum of one (1) year to be available to authorized staff for operational necessity and ready reference, subject to technical limitations.

  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 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:

- 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)

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.
    - Google Nest Cam Indoor security cameras. Deployed during Election cycle at Department of Elections in City Hall and Department's Warehouse at Pier 31.
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
    - Streams of Election processes are available to the public.
    - Streams used for line management at City Hall Vote Center is accessible by all Department of Elections staff.
    - Recordings are accessible to the following authorized staff of the Department:
        - 1092-1095 IS Administrator Series
        - 1840-1844 Management Assistant series
        - 1115 Director
        - 0951-0955 Deputy Director series
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.
    - Members of the public can register complaints / concerns or submit questions at San Francisco Department of Elections City Hall 1 Dr. Carlton B. Goodlett Place, Room 48 San Francisco, CA 94102 415-554-4375, SFVote@sfgov.org, Contact form: https://sfelections.org/sfvote/
    - The Department responds to all inquiries within 10 days of receipt, regardless of method of submission. During the election cycle, all inquiries are logged in a Public Inquiry Tracking Application, assigned to a division or staff member, and tracked to completion.
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
    - Recordings are automatically saved to Google's Cloud for a period of 10 days as part of the Nest Cam subscription plan. After 10 days, the recordings are deleted.
5. Questions & Concerns

Surveillance Impact Report

Body-Worn Cameras
Recreation and Parks

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Body-Worn Cameras.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

In line with its mission, the Department uses Body-Worn Cameras to protect the public and our staff in our parks, playgrounds and at special events. The Department can review footage for improvements in response or for training opportunities.

The Department shall use Body-Worn Cameras only for the following authorized purposes:

- Recording video and audio footage in the event of an incident. Incidents can be:
    - Actual or potential criminal conduct
    - Situation when a Park Ranger reasonably believes recordings of evidentiary value may be obtained
    - Calls for service involving a crime where the recording may aid in the apprehension/ prosecution of a suspect
Providing recording to law enforcement or other authorized persons upon request.
- Providing recording to law enforcement or other authorized persons upon request.

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is located on a park ranger. The Park Ranger must wear the body worn camera affixed to their uniform in a manner most conducive to recording both audio and video at all times. Body worn cameras are typically worn on the front of the uniform's outermost garment facing forward. Park Ranger are deployed on Park property.

Surveillance Oversight Review Dates
COIT Review: October 21, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description of Body-Worn Cameras:

- Axon Body 2 and 3 - Body Worn Cameras (BWCs): Axon Body 3 isn't just a camera: it's a rugged communications beacon front-and-center on every call. Featuring enhanced low-light performance, reduced motion blur and an LTE connection that enables real-time features like live streaming, Body 3 empowers officers with more support in the moment.

A. How It Works

To function, a Body-Worn Camera (hereinafter referred to as "surveillance technology") is a device worn by a law enforcement officer that makes an electronic audio and video recording of activities that take place during any law enforcement action. In order to function, the Park Ranger turns the body worn camera on and off. Once a Park Rangers activates the body worn camera, he/she must make every reasonable effort to have the device remain on until the incident has concluded. Park Rangers download the recordings which are saved on Evidence.com.

All data collected or processed by Body-Worn Cameras will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by Evidence.com to ensure the Department may continue to use the technology.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of [Technology name] has the following benefits for the residents of the City and County of San Francisco:

- Public safety - Protect safety of residents while promoting an open, safe and welcoming environment
- Criminal justice - Providing recording to law enforcement or other authorized persons upon request.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

The San Francisco Recreation and Park Department strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures. The Department intends to use body-worn cameras and their associated data exclusively for the authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

The administrative, technical and physical safeguards are described below:

- Administrative Safeguards: The potential impacts noted above will be included in the Departmental Body Worn Camera policy which will be administered and managed by the Chief Park Ranger. All requests for body worn camera data will be captured in a request management software solution. Data will include approved requestors of surveillance data, and inventory of all requests for Surveillance data. In addition, there will be knowledge articles describing step by step instructions on how to collect and send the data to the requestor.
- Technical Safeguards: Body worn camera data can be accessed only by the Chief Park Ranger or designee. Data is stored on Evidence.com in the cloud. Violation of the policy will be subject to standard RecPark departmental policies, which may include disciplinary action up to and including termination.
- Physical Safeguards: <p>Data is securely stored on Evidence.com in the cloud.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Body-Worn Cameras yields the following business and operations benefits:

- Staff Safety - Ensure more accountability of actions of staff
- Financial and Time Savings - Recording available so no need to do individual assessment for any incidents

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): Park Rangers (8210) [One FTE/ year - 20%]
- The one-time costs are:
    - Total Salary & Fringe: 0
    - Software: 0
    - Hardware/ Equipment: $700 per camera - 50 cameras, $1500 per charger - 10 chargers
    - Professional Services: 0
    - Training: 0
    - Other: 0
- The annual costs are:
    - Total Salary & Fringe: $15,000
    - Software: $12,000 for all cameras for licensing and storage

- Hardware/ Equipment: 0
- Professional Services: 0
- Training: 0
- Other: 0

The Department funds its use and maintenance of the surveillance technology through operational funds.

COMPARISON TO OTHER JURISDICTIONS

Body-Worn Cameras are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Body-Worn Cameras
Recreation and Parks

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 Body-Worn Cameras 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 provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Body-Worn Cameras will be used to support this mission, by describing the 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 Body-Worn Cameras, 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 Body-Worn Cameras technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Recording video and audio footage in the event of an incident. Incidents can be:
  - Actual or potential criminal conduct
  - Situation when a Park Ranger reasonably believes recordings of evidentiary value may be requested
  - Calls for service involving a crime where the recording may aid in the apprehension/ prosecution of a suspect
- Providing recording to law enforcement or other authorized persons upon request.

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

Departments 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. 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

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

In line with its mission, the Department uses body worn cameras to protect the public and our staff in our parks, playgrounds and at special events. The Department can review footage for improvements in response or for training opportunities.

In addition, Body-Worn Cameras promises to benefit residents in the following ways:

- Public safety - Protect safety of residents while promoting an open, safe and welcoming environment
- Criminal justice - Providing recording to law enforcement or other authorized persons upon request.

Body-Worn Cameras will benefit the department in the following ways:

- Staff Safety - Ensure more accountability of actions of staff
- Financial and Time Savings - Recording available so no need to do individual assessment for any incidents

To achieve its intended purpose, a Body-Worn Camera (hereinafter referred to as "surveillance technology") is a device worn by a law enforcement officer that makes an electronic audio and video recording of activities that take place during any law enforcement action. In order to function, the Park Ranger turns the body worn camera on and off. Once a Park Rangers activates the body worn camera, he/she must make every reasonable effort to have the device remain on until the incident has concluded. Park Rangers download the recordings which are saved on Evidence.com.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

Data Type	Data Format	Data Classification
- Facial images, - voice audio - location - vehicle license plate number - Additionally, Park Rangers may request personal information (e.g. name) post the incident.	MOV, AVI	Level 2

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.
- Access to recorded footage is restricted to the Chief Park Ranger or designee. Recorded footage is accessed only in response to an incident.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- Chief Park Rangers (0951)
- Lieutenant Park Ranger (8210 - Lead)

B. Members of the public, including criminal defendants

The Recreation and Parks 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

- Access limited only to Chief Park Ranger or designee. Without training or appropriate security levels in software, recordings cannot be accessed.

Data Sharing: The Recreation and Parks Department will endeavor to ensure that other agencies or departments that may receive data collected by Recreation and Parks's Body-Worn Cameras Policy 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.

The Recreation and Parks 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)

The Recreation and Parks Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Recreation and Parks 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 currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Data Type	Data Recipient
Recordings from body worn cameras	Police, Sheriff, City Attorney, District Attorney, and Public Defender

Data sharing occurs at the following frequency:

- When requested, pursuant to a subpoena.

B. External Data Sharing

Department shares the following data with the recipients:

Data Type	Data Recipient
Recordings from body worn cameras	Outside law enforcement

Data sharing occurs at the following frequency:

- When requested.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

- The Chief Park Ranger will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Body Worn Cameras.

Before data sharing with any recipient, 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.
- Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Data Retention Period	Data Retention Justification
Body worn camera recordings will be stored for a minimum of one (1) year.	This retention period allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

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.

PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- If data is associated with an incident, it may be kept for longer than the standard retention period:
  - Use of force - not deleted
  - Investigations - until case closure

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- Local Storage
- Software as a Service Product

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- Evidence.com auto-deletes after 1 year.

Processes and Applications:

- Evidence.com has a feature that allows for redaction/ de-identification. This will be performed by the Lieutenant 8210 -Lead.

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.

At the very least, 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. 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.

- Training on Evidence.com on how to view and download recordings is required.
- Evidence.com is the storage location for footage captured by Axon Body Worn Cameras.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

- The Chief Park Ranger or designee will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Body Worn Cameras.

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

- Chief Park Ranger (0951) or designee - Lieutenant (8210 - Lead).

Sanctions for violations of this Policy include the following:

- Violation of the policy will be subject to standard RecPark departmental policies, which may include disciplinary action up to and including termination.

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

For the Public:

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks through several ways:

- Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117
- Call to the RPD Front Desk 415-831-2700
- Send an email to rpdinfo@sfgov.org

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- All calls/complaints from the public received via mail or via call to the RPD Front Desk are routed to the RPD IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the RPD IT HelpDesk which then is logged in the request management system.
- Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion.
- Review of open / closed requests occur with the CIO on a weekly basis.

For 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.

Surveillance Technology Policy

Tennis Reservations Application
Recreation and Parks Department

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 the Tennis Reservations Spotery Application 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 Recreation and Parks Department's ("Department") mission is to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Tennis Reservations Spotery Application ("Spotery Application") will be used to support this mission, by describing the 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 Spotery , 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 Spotery Application technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– Confirm that the person who reserved the booking for a tennis court is at the location at the reserved time.
– Utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the Spotery web application or as a report delivered by Spotery

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

Departments 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. 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

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

The surveillance technology allows for equitable access to our recreational sites.

In addition, the Spotery Application promises to benefit residents in the following ways:

X Health - Residents are able to book reservations for tennis courts which allow for recreational and physical activity.

The Spotery Application will benefit the department in the following ways:

X Time Savings, Staff do not need to review and research anecdotal evidence about reservation holders not utilizing the court for the reserved time.

To achieve its intended purpose, the Spotery Application (hereinafter referred to as "surveillance technology" or "Spotery") allows a reservation holder to book a tennis court up to seven days in advance. 24 hours prior to the reservation, a reminder email is sent to the reservation holder. The reminder email contains a check-in button. The reservation holder can use the check-in button on their mobile device within 15 minutes before or after the reservation time. Spotery checks the location of the reservation holder to ensure that they are within 0.1 miles of the tennis court. Spotery needs access to the reservation holder's location so "Enable Location Services" must be turned on the mobile device.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- Types of Data Collected: Name, email address, address, geolocation data
- Data Classification Level: Level 2

Geolocation is briefly accessed by the Spotery Company at the time a reservation holder checks-in. It is not stored or made accessible to the Department.

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:

- Contact information
- Data Retention
- Description of the authorized use
- Information on the surveillance technology
- Type of data collected

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Prior to accessing or using data, authorized individuals receive training and instruction regarding authorized uses. Training includes how to login and run reports.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- Chief Information Officer (0941)

- Director of Property, Permits, and Reservation (0953) or designee – Administrative Analyst(s) (1820 series)

B. Members of the public, including criminal defendants

The Recreation and Parks 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

The access is limited only to the following roles: Chief Information Officer, Director of Property, Permits and Reservations, or designee.

Data Sharing: The Recreation and Parks Department will endeavor to ensure that other agencies or departments that may receive data collected by the Recreation and Parks Department's Spotery Application will act in conformity with this Policy.

For internal 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.

The Recreation and Parks 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)

The Recreation and Parks Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Recreation and Parks 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 currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

The Chief Information Officer and the Director of Property, Permits and Reservations or designee will be responsible for enforcing the Surveillance Technology policy through recurring review of functionality and use.

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

Before data sharing with any recipient, the Department will confirm the purpose of the data sharing aligns with the department's mission to ensure appropriate data protections are in place.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	**Retention Justification**
Report Downloaded from Spotery (see Appendix A for example report)- These are manually downloaded from the web application by Department staff and are saved on the file server. These will be stored for up to 1 year. Geolocation – Spotery briefly accesses geolocation as determined by the application user's mobile device Global Positioning System (GPS) at the time the user checks-in to tennis reservation. This data is not made accessible to the department.	Reports - This retention period allows for ample time for staff to analyze data regarding reservation holder usage and can determine if there were any violations to Department policy. Geolocation data is only accessed to determine that the user is within 0.1 miles of the tennis court and to update reservation status (see Appendix A for sample data). Geolocation data is not stored by Spotery and is never accessed by the Department (see Appendix B for Spotery Privacy Policy).

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.

Data collected in the Spotery Application reports downloaded by the Department is stored and safeguarded in the following location:

- DT Data Center

- Spotery's Privacy Policy (Appendix B) provides information on how the Spotery Company safeguards data

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- Reports (See Appenda A for sample report) - these are manually downloaded from the Spotery web application by Department staff and are saved on the file server. These will be stored for up to 1 year and deleted in an automated process.

- Geolocation Data - No geolocation data is provided to the Department. Spotery Application temporarily accesses geolocation data but does not retain ongoing (see Spotery Privacy Policy in Appendix B).

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.

At the very least, 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. 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.

Training is required for authorized individuals to use or access the information collected. Prior to accessing or using data, authorized individuals receive training and instruction regarding authorized uses. Training includes how to login and run reports.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Chief Information Officer and the Director of Property, Permits and Reservations or designee will be responsible for enforcing the Surveillance Technology policy through recurring review to ensure data is used only for the approved use cases: (a) Confirmation that the person who reserved the booking for a tennis court is at the location at the reserved time; (b) Utilization of data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the Spotery web application or as a report delivered by Spotery.

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

> Chief Information Officer (0941) and the Director of Property, Permits and Reservation (0953) or designee - Administrative Analysts (1820 series)

Sanctions for violations of this Policy include the following:

> Violation of the policy will be subject to Recreation and Parks Departmental policies, which may include disciplinary action up to and including termination.

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:

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks Department through several ways: (a) Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117; (b) Call to the Recreation and Parks Department Front Desk 415-831-2700; (c) Send an email to rpdinfo@sfgov.org; or (d) Contact 311.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response.

All calls/complaints from the public received via mail or via call to the Department Front Desk are routed to the Department IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the Department IT HelpDesk which then is logged in the request management. Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion. Review of open / closed requests occur with the CIO on a weekly basis.

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.

Appendix A: Sample of Report Downloaded by Department from the Spotery Application

Reservation	Spot	Status	Date from	Time from	Time to
2714335.	Hamilton Rec Tennis Court #2	Checked-In	3/17/2022	1:30 PM	3:00 PM
2714327.	Hamilton Rec Tennis Court #1	Canceled by User	3/17/2022	10:30 AM	12:00 PM
333369.	Hamilton Rec Tennis Court #2	Booked	5/01/2022	12:00 PM	1:30 PM

Appendix B: Spotery Privacy Policy

Last updated: March 2022

Welcome to Spotery, an online marketplace for short term rental of facilities provided by Social Solutions, LLC (the "Company", "SSL", "Spotery", "us", "our", and/or "we"). We are committed to ensure that the personal information that you share on our Site and/or Services is protected and kept confidential. By accepting the Terms of Service or providing information through our Site or mobile application, you agree to the use and disclosure of personal identifiable information, as detailed in this Privacy Policy.

I. Key Terms

Unless otherwise defined in this Privacy Policy, capitalized terms shall have the meaning set forth on the Terms of Use.

II. Information Collected

1. Information Collected from your use

We ask for and collect the following personal information about you when you use the Site. This information is necessary for the adequate performance of the contract between you and us and to allow us to comply with our legal obligations and given our legitimate interest in being able to provide and improve the functionalities of the Site and Services. Without it, we may not be able to provide you with all the requested services.

- **Account Information.** When you sign up for a Spotery Account, we require certain information such as your first name, last name, email address, and date of birth.
- **Profile and Listing Information.** To use certain features of the Site (such as booking or creating a listing), we may ask you to provide additional information, which may include your address, phone number, and a profile picture.
- **Identity Verification Information.** To help create and maintain a trusted environment, we may collect identity verification information (such as images of your government issued ID, passport, national ID card, or driving license, as permitted by applicable laws) or other authentication information.
- **Payment Information.** To use certain features of the Site (such as booking or creating a listing), we may require you to provide certain financial information (like your bank account or credit card information) in order to facilitate the processing of payments.

- **Communications with Spotery and other Members.** When you communicate with Spotery or use the Site to communicate with other Members, we collect information about your communication and any information you choose to provide.
- **Geolocation Information.** For certain features of the Site, we may capture geolocation information about your approximate location as determined by your mobile device's GPS to provide you with an enhanced user experience. Most mobile devices allow you to control or disable the use of location services for apps in the device's settings menu. We do not store geolocation data, as it is only necessary to activate certain functionalities at the time of use.
- **Usage Information.** We collect information about your interactions with the site such as the pages or content you view, your searches for Listings, bookings you have made, and other actions on the Site.
- **Log Data and Device Information.** We automatically collect log data and device information when you access and use the Site, even if you have not created a Spotery Account or logged in. That information includes, among other things: details about how you've used the Site (including if you clicked on links to third party applications), IP address, access dates and times, hardware and software information, device information, device event information, unique identifiers, crash data, cookie data, and the pages you've viewed or engaged with before or after using the Site.
- **Cookies and Similar Technologies.** We use cookies and other similar technologies when you use our platform, use our mobile app, or engage with our online ads or email communications. We may collect certain information by automated means using technologies such as cookies, web beacons, pixels, browser analysis tools, server logs, and mobile identifiers. In many cases, the information we collect using cookies and other tools is only used in a non-identifiable without reference to personal information. For example, we may use information we collect to better understand website traffic patterns and to optimize our website experience. In some cases, we associate the information we collect using cookies and other technology with your personal information. Our business partners may also use these tracking technologies on the Site or engage others to track your behavior on our behalf.
- **Pixels and SDKs.** Third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from our websites and elsewhere on the internet and use that information to provide measurement services and target ads. For apps, that third parties, including Facebook, may collect or receive information from your app and other apps and

use that information to provide measurement services and targeted ads. Users can opt-out of the collection and use of information for ad targeting by updating their Facebook account ad settings and by contacting support@spotery.com with a description of your request and validation information.

- **Total Fee Payment Transactions.** We collect information related to your payment transactions through the Site, including the payment instrument used, date and time, payment amount, payment instrument expiration date and billing postcode, email address, IBAN information, your address and other related transaction details. This information is necessary for the adequate performance of the contract between you and Spotery.

2. Information Collected from you from third parties

- **Third Party Services.** If you link, connect, or login to your Spotery Account with a third party service (e.g. Google, Facebook), the third party service may send us information such as your registration, friends list, and profile information from that service. This information varies and is controlled by that service or as authorized by you via your privacy settings at that service.
- **Background Information.** To the extent permitted by applicable laws, Spotery may obtain reports from public records of criminal convictions or sex offender registrations.
- **Referrals.** If you are invited to Spotery, the person who invited you may submit personal information about you, such as your email address or other contact information.
- **Other Sources.** To the extent permitted by applicable law, we may receive additional information about you, such as demographic data or information to help detect fraud and safety issues, from third party service providers and/or partners, and combine it with information we have about you. For example, we may receive background check results (with your consent where required) or fraud warnings from service providers like identity verification services for our fraud prevention and risk assessment efforts. We may receive information about you and your activities on and off the site through partnerships, or about your experiences and interactions from our partner ad networks.

III. Use and Sharing of Information Collected

Your acceptance of the Terms of Service and this Privacy Policy grant Spotery a worldwide non-exclusive, transferable, irrevocable, sublicensable, royalty-fee license to use your personal information for the purposes set forth herein and as permissible under applicable laws or regulations. By accepting the Privacy Policy and the Terms of Service, you understand our policies and practices regarding your personal information and how we will treat it.

We may use, store, and process personal information to (1) provide, understand, improve, and develop the Site, (2) create and maintain a trusted and safer environment (such as to comply with our legal obligations and ensure compliance with our policies) and (3) provide, personalize, measure, and improve our advertising and marketing.

We process this personal information for these purposes given our legitimate interest in improving and protecting the Site and our Members' experience with it, and where it is necessary for the adequate performance of the contract with you and to comply with applicable laws. We will also process your personal information for the purposes listed in this section, given our legitimate interest in undertaking marketing activities to offer you products or services that may be of your interest.

We may share your personal information for one or more of the following reasons:

- **Social media**

  Where permissible according to applicable law we may use certain limited personal information about you, such as your email address, to hash it and to share it with social media platforms, such as Facebook or Google, to generate leads, drive traffic to our websites or otherwise promote our products and services or the Site. These processing activities are based on our legitimate interest in undertaking marketing activities to offer you products or services that may be if your interest.

  The social media platforms with which we may share your personal information are not controlled or supervised by Spotery. Therefore, any questions regarding how your social media platform service provider processes your personal information should be directed to such provider.

- **Members**

  To help facilitate bookings or other interactions between Members, we may need to share certain information, including personal information but excluding financial information, with other Members, as it is necessary for the adequate performance of the contract between you and us

- **Affiliated parties**

  To enable or support us in providing the Site and Services, we may share your information, including personal information, within our corporate family of companies (both financial and non-financial entities) that are related by common ownership or control.

- **Compliance with Law and Government Requirements**

  Spotery may disclose your information, including personal information, to courts, law enforcement, governmental authorities, tax authorities, or authorized third parties, if and to the extent we are required or permitted to do so by law or if such disclosure is reasonably necessary:

  (i) to comply with our legal obligations, (ii) to comply with a valid legal request or to respond to claims asserted against Spotery or its affiliated parties, (iii) to respond to a valid legal request relating to a criminal investigation or alleged or suspected illegal activity or any other activity that may expose us, you, or any other of our users to legal liability, (iv) to enforce and administer our Terms of Service or other policies and agreements with Members, or (v) to protect the rights, property or personal safety of Spotery, its employees, its Members, or members of the public.

  Where appropriate, we may notify Members about legal requests unless: (i) providing notice is prohibited by the legal process itself, by a court order we receive, or by applicable law, or (ii) we believe that providing notice would be futile, ineffective, create a risk of injury or bodily harm to an individual or group, or create or increase a risk of fraud upon Spotery's property, its Members and the Site. In instances where we comply with legal requests without notice for these reasons, we may attempt to notify that Member about the request after the fact where appropriate and where we determine in good faith that we are no longer prevented from doing so.

  In jurisdictions where Spotery facilitates or requires a registration, notification, permit, or license application of a Facility Owner or Service Provider with a local governmental authority through the Site in accordance with local law, we may share information of participating Facility Owners or Service Provider with the relevant authority, both during the application process and, if applicable, periodically thereafter.

In jurisdictions where Spotery facilitates the Collection and Remittance of Occupancy Taxes where legally permissible according to applicable law, expressly grant us permission, without further notice, to disclose Members' data and other information relating to them or to their transactions, bookings, Accommodations and Occupancy Taxes to the relevant tax authority.

- **Service Providers**

  Spotery uses a variety of third-party service providers to help us provide services related to the Site and the Services. Spotery will require compliance with the laws from said third parties. But you as a user must understand that Spotery is not responsible for the privacy practices of any third-party service provider, nor for their acts or omissions.

IV. Security

We are continuously implementing and updating administrative, technical, and physical security measures to help protect your information against unauthorized access, loss, destruction, or alteration. Some of the safeguards we use to protect your information are firewalls and data encryption, and information access controls. If you know or have reason to believe that your Spotery Account credentials have been lost, stolen, misappropriated, or otherwise compromised or in case of any actual or suspected unauthorized use of your Spotery Account, please contact us following the instructions in the Contact Us section below.

V. Severability

All personal information collected will be secured in accordance with the policies in force at the time of its collection. If any of these conditions is considered invalid, void or for any reason unenforceable, that condition will be considered severable and will not affect the validity and enforceability of any remaining conditions.

VI. Modifying or deleting your personal information

If you wish to modify your personal information, or if you wish to discontinue receiving materials from us or wish to remove your personal information from Spotery's database, you can contact us at s upport@spotery.com. Please allow up to 72 hours to process your request.

VII. Personal data retention

We retain personal data only for as long as is needed to exercise our legal obligations and for appropriate business purposes.

If you contacted us to delete your data, Spotery may retain limited aggregate information for research purposes and to help us further improve our services and exercise our legal obligations.

This aggregate information does not include any personal data that relates to you as an individual.

VIII. Changes to the Privacy Policy

In the future, we may modify our Privacy Policy. In case of changes, we will make sure to publish them on the Site and in other places that we consider appropriate.

CONTINUING USING THE SITE AFTER PUBLICATIONS REGARDING CHANGES OR MODIFICATIONS TO THE PRIVACY POLICY CONSTITUTES AN ACCEPTANCE BY THE USER OF SUCH CHANGES OR MODIFICATIONS. IF USER DISAGREES WITH THE CHANGES OR MODIFICATIONS, THE USER MUST IMMEDIATELY WITHDRAW FROM THE USE OF THE SITE.

IX. Questions

If you have any questions regarding our Privacy Policy, email us at info@spotery.com.

Surveillance Impact Report

Spotery - web application used for tennis reservations
Recreation and Parks Department

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Spotery - web application used for tennis reservations.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well- being of our diverse community.

In line with its mission, the Department uses Spotery to allow for equitable access to our recreational sites.

The Department shall use Spotery only for the following authorized purposes:

- To confirm that the person who reserved the booking for a tennis court is at the location at the reserved time
- To utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the web application or as a report delivered by Spotery.

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Department technology is located as an app through Spotery. The reservation holder can use the check in button (sent by the reservation system) within 15 minutes before or after the reservation time. Spotery checks the location of the reservation holder to ensure that they are within 0.1 miles of the tennis court reserved. If not, the check in process cannot be completed.

Technology Details

The following is a product description of Spotery:

Spotery's core business is a marketplace for facility rentals. San Francisco Recreation & Park Department (SFRPD) Permits & Reservations worked with Spotery to custom build a reservation platform for tennis courts so that these could be fairly allocated (please see: https://www.spotery.com/).

A. How It Works

To function, Spotery works as reservation holder to allow a person to book a tennis court up to seven days in advance.

Surveillance Oversight Review Dates
COIT Review: June 16, 2022
Board of Supervisors Review: TBD

24 hours prior to the reservation, a reminder email is sent to the reservation holder. The reminder email contains a check-in button. The reservation holder can use the check in button within 15 minutes before or after the reservation time.

Spotery checks the location of the reservation holder to ensure that they are within .1 miles of the tennis court. Spotery needs access to the reservation holder's location so "Enable Location Services" must be turned on.

All data processed by Spotery will be handled by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by Social Solutions to ensure the Department may continue to use the technology.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of Spotery has the following benefits for the residents of the City and County of San Francisco:

X Health - Residents are able to book reservations for tennis courts which allow for recreational and physical activity.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

- The San Francisco Recreation and Park Department strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures. The Department intends to use the Spotery GPS check in and associated data exclusively for the authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

  The administrative, technical and physical safeguards are described below.

- Administrative Safeguards: Only the Chief Information Officer (0941) and the Director of Property, Permits and Reservation (0953) or designee - Administrative Analysts (1820 series) will have logins to the Spotery web app to access the data.
- Technical Safeguards: Only the Chief Information Officer (0941) and the Director of Property, Permits and Reservation (0953) or designee - Administrative Analysts (1820 series) will have logins to the Spotery web app to access the data. Data is encrypted and sent via SSL.
- Physical Safeguards: Data is securely stored by Spotery in the cloud.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Spotery yields the following business and operations benefits:

X Time Savings, Staff do not need to review and research anecdotal evidence about reservation holders not utilizing the court for the reserved time.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): 1 FTE - Senior Administrative Analyst (1823) - 25%
- The annual costs are:
    - Total Salary & Fringe: $42k Based on: 1823 Salary (127k) * Fringe (.33) * % Time Spent (.25)
    - Software: $15k for all functionality offered by Spotery (include the GPS Check in feature)
    - Hardware/ Equipment: 0
    - Professional Services: 0
    - Training: 0
    - Other: 0

The Department funds its use and maintenance of the surveillance technology through operational funds.

COMPARISON TO OTHER JURISDICTIONS

Spotery is currently utilized by other governmental entities for similar purposes.

Surveillance Impact Report

Automated License Plate Readers ("ALPR")
San Francisco Municipal Transportation Agency - SFMTA

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

This Surveillance Impact Report details the benefits, costs, and potential impacts associated with the use of Automated License Plate Readers ("ALPR") technology by the San Francisco Municipal Transportation Agency ("Department").

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to connect San Francisco through a safe, equitable, and sustainable transportation system.

In line with its mission, the Department uses ALPR technology to efficiently enforce State parking and other vehicle laws and to calculate parking fees in City-owned parking facilities. These uses support the Department's mission because they help ensure the sustainability of and more equitable access to the City's limited parking resources, which are part of its larger transportation system.

The Department shall use ALPR technology only for the following authorized purposes:

Authorized Use(s):

1. Enforcing parking restrictions and laws.
2. Traffic Only Lane Enforcement (TOLE).
3. Link individual vehicles to their times of entry/exit into City-owned parking garages to accurately calculate parking fees.
4. Identify vehicles that are the subject of an active investigation by the SFPD (e.g., vehicles included on "hot lists" generated by the SFPD –see Appendix B & C, page 8 of SFPD ALPR Policy).
5. Analysis and reporting on parking and curb usage.

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

ALPR technology may be deployed in the following locations, based on Authorized Use(s):

System	Description
Parking Enforcement	Mobile ALPR cameras installed on Parking enforcement vehicles.
Parking Garage	ALPR technology located at entry and exits points in City-owned parking garages and lots. Geographic locations are available on Department's website.
Transit Only Lane Enforcement (TOLE):	Department plans to add Genetec ALPR cameras on busses, trolleys, and LRVs for TOLE.

Surveillance Oversight Review Dates
COIT Review: October 21, 2021
Board of Supervisors Review: TBD

Technology Details

ALPRs are high-speed camera systems that photograph vehicle license plates, convert the numbers and letters into machine-readable text, tag them with the time and location stamps, and upload that data into a database for later retrieval.

How It Works

The Department uses ALPR cameras for the purposes, described below.

- **Parking Enforcement:** The Department's current ALPR system used for parking enforcement consists of Genetec AutoVu Sharp IP-based ALPR cameras with onboard processing and the AutoVu Standard Software package. The cameras are Sharp V, AutoVu cameras mounted on the roofs of parking enforcement vehicles and wheel focused cameras on the sides of the vehicles. The roof top mounted cameras read the license plates and the side mounted cameras photograph the wheel/tire to compare on the second pass for time-limited enforcement. The system utilizes the Genetec software to create the user interface and in-vehicle mapping. The system utilizes cellular communication to transmit reads to the backend software. The backend software consists of the Genetec Security Center software to manage access to all uploaded plate reads, hotlists, and user-level access credentials.

  ALPR data collected for parking enforcement purposes is currently handled and/or stored by Genetec, a third-party vendor.

- **Transit Only Lane Enforcement (TOLE):** The Department plans to deploy the Genetec ALPR system it uses for parking enforcement purposes on its transit vehicles for Transit Only Lane Enforcement (TOLE). The Department currently reviews video footage manually looking for violations. A pilot program is planned for the third quarter of 2021. ALPR cameras will be installed in front of transit vehicles to enforce TOLE violations (e.g., driving or stopping in transit only lanes or blocking bus stops), but only when operating inside specified enforcement zones within the City.

  ALPR data collected for TOLE will not be handled or stored by a third-party vendor. The Department will remain the sole custodian of record.

- **Parking Garages:** Fixed cameras are mounted inside City-owned parking garages and lots. Cameras are triggered only when vehicles are moving over an arming loop, and cameras are positioned to focus only on license plates. The highly reliable, compact VRS-N60E Imaging unit features state-of-the-art hardware along with HTS's powerful, patented PC-based license plate recognition (LPR) and VRS-See Control management software. The hardware is optimized specifically for high performance with HTS software applications. With its built-in VRS Controller Application, the VRS-N60E provides maximum effectiveness as it's specifically engineered for optimal accuracy, confidence, and vehicle recognition solutions. HTS Imaging Units and value-added HTS solutions are field proven in over 40 countries worldwide, including the United States. Sophisticated HTS algorithms identify both the state and country of any license plate.

ALPR data collected in parking garages or lots are not handled or stored by an outside provider or third-party vendor. The Department is the sole custodian of record.

IMPACT ASSESSMENT

This impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

A. The benefits of the surveillance technology outweigh the costs.
B. The Department's Policy safeguards civil liberties and civil rights.
C. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of ALPR technology has the following benefits for the residents of the City and County of San Francisco:

☐	Education	
☑	Community Development	Informs planning, policy development, and pricing for public parking spaces (e.g., for specific commercial districts).
☐	Health	
☑	Environment	Improves street conditions by ensuring timely turnover of parking spaces for use by city residents and visitors.
☑	Criminal Justice	Identifies vehicles reported to, and that are subject to, an active investigation by the SFPD.
☐	Jobs	
☐	Housing	
☑	Other	Helps ensure timely turnover of parking spaces, giving city residents and visitors more equitable access to limited parking resources. Ensures customers with lost tickets pay the actual value of their vehicle's stay in the parking garage.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

- **Dignity Loss:** Technical safeguards make this impact (e.g., embarrassment and emotional distress) unlikely because ALPR cameras take photos of vehicles, primarily their license plates; they do not capture images of vehicle occupants. Occasionally, images may include pedestrians who are near license plates, but these images are accidental and are purged from the ALPR system.
- **Discrimination:** Technical safeguards make this impact (i.e., unfair or unethical differential treatment of individuals or denial of civil rights) highly unlikely because ALPR applies the policies and regulations equally to all vehicles. ALPR is used to enforce time-limited parking regulations and identify scofflaw (i.e., vehicles with five or more delinquent parking citations) and stolen vehicles. As to time-limited parking enforcement, administrative safeguards make this impact minimal because ALPR technology is deployed equally in areas throughout the City where restrictions apply, and such restrictions are typically requested by the majority of residents in the corresponding communities. As to scofflaw and stolen vehicles, administrative safeguards make this impact minimal because ALPR technology is deployed for this purpose throughout the SFMTA's jurisdiction.
- **Economic Loss:** Technical safeguards make this impact (e.g., identify theft/misidentification) minimal because the ALPR system has no access to information identifying individuals, including vehicle owners or drivers. ALPR mitigates economic losses to customers of City-owned parking facilities by calculating the exact parking fees owned even in cases of lost tickets in Department owned parking facilities.
- **Loss of Autonomy:** Technical safeguards make this impact (e.g., loss of control over decisions on how personal information is used or processed) highly unlikely because the ALPR system has no access to information identifying individuals, including vehicle owners or drivers. Moreover, since data is processed mostly by the ALPR system, there is minimum human interaction.
- **Loss of Liberty:** Administrative safeguards make this impact (i.e., improper exposure to arrest or detainment due to incomplete or inaccurate data) highly unlikely because SFPD validates data (i.e., they confirm vehicles they seek are in parking garages associated with corresponding license plates) before taking any action.
- **Physical Harm:** Technical safeguards make this impact (e.g., physical harm or death) highly unlikely because the ALPR system has no access to information identifying individuals.
- **Loss of Trust:** Department limits access to the data to only authorized users. Technical safeguards make this impact (e.g., breach of implicit or explicit expectations or agreements about the processing of data, or failure to meet subjects' expectation of privacy for information collected) minimal because license plate numbers are used to identify vehicles for purposes of determining parking fees, parking violations, scofflaws, and whether they are on a SFPD hotlist.

Fiscal Analysis of Costs and Benefits

The Department's use of Automated License Plate Readers ("ALPR") yields the following business and operations benefits:

Benefit		Description
☑	Financial Savings	Minimizes physical chalking by Parking Control Officers (PCOs); chalking can cause repetitive motion injuries, which result in workers compensation claims filed against The City.
☑	Time Savings	Helps PCOs cover larger geographic areas and improves effectiveness and efficiency in performing their duties.
☑	Staff Safety	Parking staff no longer required to work within confined areas in parking garages. Also, minimizes repetitive motion injuries from physical chalking by automating the process for Parking Control Officers (PCOs) to mark vehicles.
☑	Data Quality	Improves accuracy and simplifies parking enforcement duties. Improves data required to calculate parking fees, especially when patrons lose their parking tickets within Department owned garages.
☑	Other	Provides higher volumes of data about parking utilization, which informs planning and policy development.

The fiscal cost, such as initial purchase, personnel, and other ongoing costs of using ALPR technology includes:

FTE (new & existing)	None. Department staff uses the ALPR data, however, maintenance and support has been outsourced.	
Classification	Users are listed in our policy in section Access A.	
	Annual Cost	***One-Time Cost***
Software		$13,500
Hardware/Equipment		$1,007,181
Professional Services		$17,500
Training		*$850*
Other		$26,500
Total Cost		*$1,065,531*

2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.).
SFMTA Capital Improvement Project (CIP) Budget for initial system; SFMTA Operating Budget for ongoing operations.

The Department funds its use and maintenance of ALPR technology through general operations budget and occasional grants

COMPARISON TO OTHER JURISDICTIONS

ALPR technology is currently used by other governmental entities for purposes similar to the Department's. These government entities include the cities of Alameda, Berkeley, Emeryville, Foster City, Oakland, Palo Alto, Sacramento, San Jose, San Mateo and Santa Clara.

Surveillance Technology Policy

Automated License Plate Readers ("ALPR")
San Francisco Municipal Transportation Agency - SFMTA

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, this Surveillance Technology Policy (Policy) aims to ensure the responsible use of Automated License Plate Readers (ALPR) itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties by the San Francisco Municipal Transportation Agency (Department). This Policy complies with the requirements for the collection of license plate information set forth in Civil Code section 1798.90.5 *et seq*) and, in accordance with such law, is posted on the Department's website at: https://www.sfmta.com/about-us/sfmta-board-directors/sfmta-policies/automated-license-plate-recognition-policy.

PURPOSE AND SCOPE

The Department's mission is to connect San Francisco through a safe, equitable, and sustainable transportation system.

This Policy describes the manner in which the Department uses or will use ALPR technology to support this mission, by describing the technology's intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all Department personnel that use, plan to use, or plan to procure ALPR technology, including employees, consultants, contractors, and vendors. Employees, consultants, contractors, and vendors while working for or on behalf of the City, with the Department, are required to comply with this Policy.

POLICY STATEMENT

The authorized uses of ALPR technology for the Department are limited to the following use cases and are subject to the requirements set forth in this Policy.

Authorized Use(s):

1. Enforce parking restrictions and laws.
2. Transit Only Lane Enforcement (TOLE).
3. Link individual vehicles to their times of entry/exit into City-owned parking garages and lots to accurately calculate parking fees.
4. Identify vehicles that are the subject of an active investigation by the SFPD (e.g., vehicles included on "hot lists" generated by the SFPD – see Appendix B & C of SFPD ALPR Policy, also attached to this policy).
5. Analysis of and reporting on parking and curb usage.

Prohibited uses of ALPR technology include uses not described in the Authorized Use(s) above.

The Department may use information or data collected from ALPR technology (ALPR data) only for authorized purposes and not to 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, The Department may not use ALPR technology to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

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

- Ensures efficient enforcement of parking restrictions and laws while aiding in the calculation of parking fees, and timely turnover of parking spaces. These uses support the Department's mission because they help ensure the sustainability of and more equitable access to the City's limited parking resources, which are part of its larger transportation system.
- Links parking tickets to vehicles parked in City-owned garages and lots to calculate customer-specific parking fees. This use supports the Department's mission because it maximizes the integrity of parking revenues, which the Department uses to fund elements of the City's larger transportation system, including transit.
- Allows the Department to efficiently enforce Transit Only Lanes which is in alignment with San Francisco's Transit-First Policy.

In addition, ALPR technology benefits residents in the following ways:

☐	Education	
☑	Community Development	Informs planning, policy development, and pricing for public parking and loading spaces (e.g., for specific commercial districts).
☐	Health	
☑	Environment	Improves street conditions by ensuring timely turnover of parking spaces for use by City residents and visitors.
☑	Criminal Justice	Identifies vehicles reported to, and that are subject to, an active investigation by the SFPD.
☐	Jobs	
☐	Housing	
☑	Other	Ensures customers with lost tickets are charged the actual value of their vehicle's stay in City-owned parking garages and lots instead of the maximum rates.

ALPR technology will benefit the Department in the following ways:

Benefit		Description
☑	Financial Savings	Minimizes physical chalking by Parking Control Officers (PCOs); chalking can cause repetitive motion injuries, which result in workers compensation claims filed against The City.
☑	Time Savings	Helps PCOs cover larger geographic areas and improves effectiveness and efficiency in performing their duties.
☑	Staff Safety	Parking garage staff no longer required to work within confined areas in parking garages. Minimizes repetitive motion injuries from physical chalking by automating the process for PCOs to mark vehicles.
☑	Data Quality	Improves accuracy and simplifies parking enforcement duties. Provides data required to calculate parking fees, especially when patrons lose their parking tickets within City-owned parking garages and lots. Provides data to inform potential new on-street parking and curb policies and regulations.
☑	Other	Provides anonymized data about parking and curb utilization, which informs planning and policy development.

POLICY REQUIREMENTS

This Policy describes the Department's data management processes and safeguards to ensure transparency, oversight, and accountability in its use of ALPR technology and ALPR data. The Department's use of ALPR technology, including its collection, retention, processing, and sharing of ALPR data must comply with this Policy and with all applicable City, State, and Federal laws.

Specifications:	The software and/or firmware used to operate the ALPR technology must be up to date and maintained.
Safety:	ALPR technology must be operated in a safe manner. ALPR technology will not be operated in a way that infringes on civil rights of residents or visitors, including their privacy rights, or that causes personal injury or property damage.
Data Collection:	The Department will minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the APLR technology.

The Department will collect ALPR data only as required to execute the authorized uses of ALPR technology. All ALPR data collected, including PII, if any, will be classified according to the City's Data Classification Standard.

The Department shall remove from the raw data it collects using ALPR technology any incidental data that may be used to identify persons or private information, including any PII, that is not necessary to accomplish the intended purpose of the ALPR technology.

ALPR data includes the following data types:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	JPEG, G64m	Level 3
Date and Time	SQL or proprietary	Level 3
Geolocation data	SQL	Level 3

Notification: Where reasonably possible given access and safety considerations, the Department will provide notice to the public of its operation of ALPR technology through signage located in viewable public areas. These notices will state the purpose of the ALPR technology being used at the applicable site(s)

The Department's signs will include the following information (as applicable) about the ALPR technology:

- ☑ Description of the technology used
- ☑ Description of the authorized use(s) or purpose(s)
- ☐ Type of data collected
- ☐ Whether persons be individually identified
- ☐ Data retention schedule
- ☑ Department's name
- ☑ Department's contact information

Access: Persons with access to ALPR data must adhere to the following rules and processes:

- Authorized users must complete mandatory training and obtain login credentials.
- Only authorized users may use ALPR technology or access ALPR data.
- Authorized users must log into tablet or computer, as applicable, to access ALPR data.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use ALPR data that is collected, retained, processed, or shared:

- 104x – IT Staff
- 109x – Operations Support Admin
- 182x – Administrative Analyst
- 184x - Management Assistant
- 917x - Managers

- 5277 – Planner I
- 5288 – 5290 Transportation Planners
- 8214 – Parking Control Officer(s)

B. Members of the public, including criminal defendants

With respect to public access to ALPR data, the Department will comply with applicable law, including the California Public Records Act and San Francisco Sunshine Ordinance.

Data Security: The Department will secure any PII against unauthorized access, processing, disclosure, and accidental loss, destruction, or damage. ALPR data collected and retained by the Department will be protected by the safeguards appropriate for its classification level(s).

To protect ALPR data from unauthorized access and control, including misuse, the Department shall, at minimum, apply the following safeguards:

- Authorized users require unique login credentials to access ALPR technology, which is accessible on portable tablets and on workstations.
- All access to and activity in the ALPR system is logged and can be audited.

Data Sharing: The Department will endeavor to ensure that other agencies or departments with which it shares ALPR data receive a copy of and comply with this Policy.

The Department will ensure administrative, technical, and physical safeguards are in place before sharing ALPR data internally with other City departments and with entities outside the City (e.g., other government entities, contractors, vendors). (See Data Security).

Before sharing ALPR data that contains personal information outside the Department, if reasonably possible, the Department will take measures (e.g., de-identification, anonymization, aggregation, etc.) to protect the identities of individuals.

Further, in sharing ALPR data, the following shall be prohibited: (1) the processing of personal data to reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and (2) the processing of genetic data or biometric data to identify an individual person. Sharing data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Before sharing ALPR 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 applicable 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 applicable law, including San Francisco's Sunshine Ordinance.

☑ Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

This Policy authorizes the Department's data sharing practices, as follows:

A. Internal Data Sharing

The Department may share ALPR data with the following recipients internal to the City and County of San Francisco:

- Different divisions with the Department
- Police Department
- City Attorney
- District Attorney
- Sheriff

Data sharing with these internal recipients occurs at the following frequency:

- As needed.

B. External Data Sharing

The Department may share ALPR data with the following recipients external to the City and County of San Francisco:

- City-owned parking garage operators under contract with the Department (currently, LAZ and Impark/IMCO).
- Vendors under contract with the Department to support or maintain the ALPR technology and its associated data to ensure it remains functional (currently Conduent Technology, citation-processing contractor). Hardware manufacturers Genetec (ALPR vendor), and Skidata (parking access and revenue control system (PARCS) vendor).

Parking garage operators and vendors, listed above, may change periodically as their contracts expire and as they are acquired or merge with new business entities. Their function, however, will remain substantially the same.

Data sharing with these external recipients occurs at the following frequency:

- Ongoing

To ensure external entities receiving data collected by ALPR technology comply with this Policy, Department shall:

- Ensure they receive a copy of and comply with this Policy.

Data Retention:

The Department's ALPR data retention schedule, by data type, and justification are as follows:

Type of Data	Justification for Retention
Digital images not associated with a parking citation are retained for 14 days.	To allow enforcement of 120-hour parking restrictions – PCOs require images taken at least 72 hours apart to enforce restrictions.
Digital images associated with a parking citation are retained for 365 days.	To support validity of contested parking citations at Department Administrative Hearings.
Digital images from parking garages are retained for 60 days after customer exists garage.	To assist SFPD in investigations of vehicular break-ins (consistent with maximum period the California Highway Patrol can retain ALPR data under state law (CVC 2413(b))).
Parking garage data (digital images converted to numerical data) stored for archive reporting 2 years.	Parking garage data is stored 2 years for auditing purposes. This includes parking taxes information for the tax collector's office. It is not meant for garage utilization or demand planning.
If license plate is used as a credential for entry and exit into parking garage (e.g., frictionless parking or reservation) license plate information is stored for as long as individual is using that service.	To allow customers access to parking garage for the duration of their reservation or use period. (License plate information is used in instead of an access card to grant access.)

The Department will store and retain raw PII it collects with ALPR technology only as long as necessary to accomplish a lawful purpose authorized under this Policy. PII collected by ALPR technology may be retained beyond the applicable retention period(s), above, only in the following circumstance(s):

- Where ALPR data is used in a criminal investigation, or as otherwise required by law.

Departments must establish appropriate safeguards for PII data stored for longer periods.

ALPR Data will be stored in the following location(s):

☑ Local storage
☑ Department's Data Center
☐ Software as a Service Product
☑ Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, the Department shall dispose of ALPR data in the following manner:

Practices:

- Upon completion of the applicable data retention period, the Department will automatically dispose of raw ALPR data (e.g., ALPR data that has not been anonymized or aggregated).

Training: To reduce the risk that ALPR technology or ALPR data will be used in a way that violates this Policy, individuals requiring access to ALPR technology or ALPR data must receive training on data security policies and procedures.

At minimum, the Department shall require all employees, consultants, contractors, vendors, and volunteers working with ALPR technology on its behalf to read and acknowledge all authorized and prohibited uses. The Department shall also require that individuals with access to PII receive appropriate training before being granted access to systems containing PII.

The Department will ensure employees and vendors are trained on how to use the ALPR technology correctly and ensure ALPR data is used for its intended use only. Training includes explaining how employees and vendors can use data and how to report problems with the ALPR system.

COMPLIANCE

The Department shall oversee and enforce compliance with this Policy using the following methods:

- The Department will assign the positions listed below to oversee, or assign staff members under their direction to oversee, compliance with this Policy.
  - Commander of Parking Enforcement and Traffic.
  - Operations Manager, SFMTA Parking and Curb Management.
  - Policy Manager, SFMTA Parking and Curb Management.

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 include written warning, suspension, and termination of employment.

EXCEPTIONS

The Department may use ALPR technology or ALPR data in ways that may be inconsistent with this Policy in the following cases: (1) to respond to exigent circumstances; or (2) if ordered by a court or otherwise required by law.

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 ALPR technology or ALPR data.

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:

Public complaints or concerns may be submitted to the Department by:

- All complaints or concerns should be routed through 311.org.

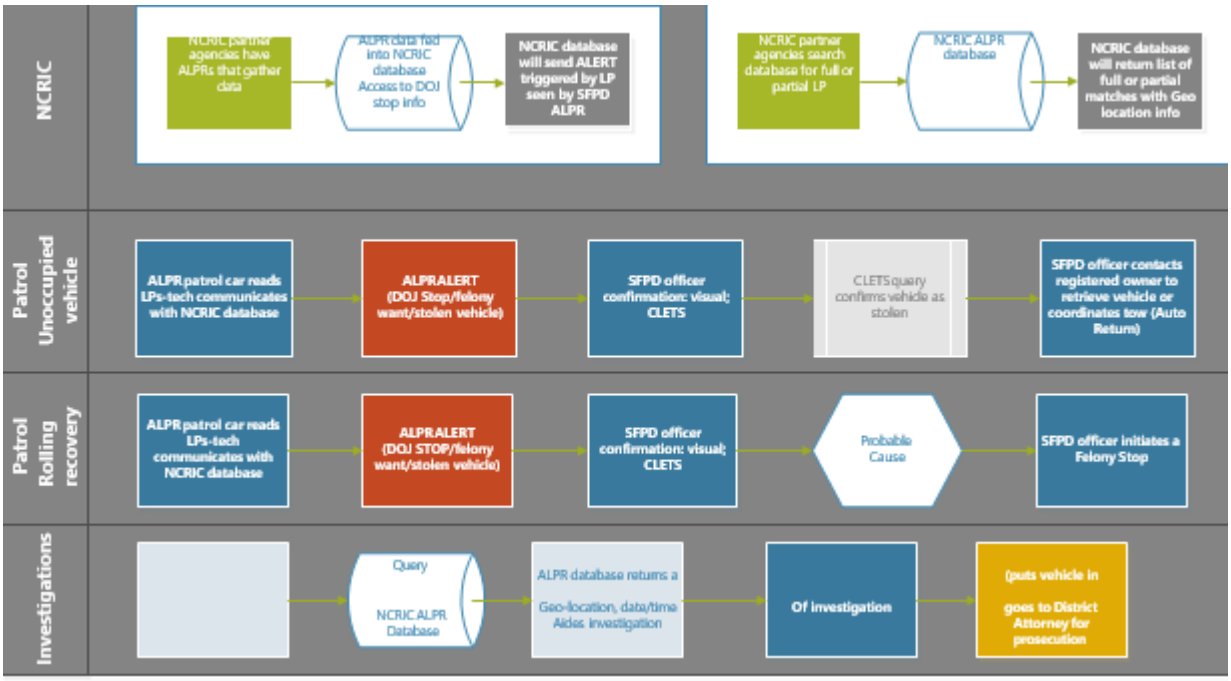
The Department shall acknowledge and respond to complaints and concerns in a timely and organized manner. In so doing, Department shall:

- Respond to 311 within required Service Level Agreement (SLA).

City and County of San Francisco Employees:

All questions from Department employees regarding this Policy should be directed to the employee's supervisor or one of the persons identified in the **COMPLIANCE** section, above, with oversight responsibilities. Similarly, questions about other applicable laws governing the use of the ALPR technology or the issues related to privacy should be directed to the employee's supervisor or the director.

APPENDIX A: SFPD Use of ALPR Data



Appendix B: "Hot List" or "Hot Sheets" Definition Relating to ALPR Data Accessed by SFMTA

Stolen vehicles and stolen plates in the City and County of San Francisco as reported through Police Incident Reports and available through CABLE/CLETS

Appendix C: "Hot Lists" Categories That May Trigger ALPR Alerts, If ALPR Technology Is So Configured

For SFPD ALPR usage, "Hot List" refers to license plates that are associated with "DOJ Stop/Felony Wants". "DOJ Stop/Felony Want" are listed as follows:

- Stolen Vehicles
- Stolen Plates
- Felony Wants (Homicide, Domestic Violence, Kidnapping, Aggravated Assault, shootings etc.)
- Missing Person
- Protection Order
- Sex Offenders
- Canadian Stolen Plate
- Violent Gang Terrorist Organization File (VGTOF)
- Violent Offender
- Wanted Persons

Surveillance Impact Report

Taxi Dashboard Camera
Municipal Transportation Agency

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of limited video file(s) received from Taxi Dashboard Cameras.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to connect San Francisco through a safe, equitable, and sustainable transportation system.

In line with its mission, the Department uses the video files from the Taxi Dashboard Cameras for the following: Taxi Dashboard Camera's are owned by the taxi cab companies and are not governed by Department's surveillance policies.

Taxis are one of several modes of transportation the Department regulates within the City. Taxi cab companies and other taxi permittees that operate in the City are subject to a number of requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transp. Code to ensure safety, equity of service, and sustainability among other goals.

The Department shall use the video data from Taxi Dashboard Cameras only for the following authorized purposes:

– Review recording of on-board incidents based upon complaints received from the public and at appeals hearing in response to a fine, suspension or response to fine revocation.
– Review video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transportation Code.
– Review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides. For example, under its wheelchair program taxi incentive, the Department reviews video data from the technology to confirm that taxi cab drivers pick up individuals with certain disabilities before paying drivers for those rides, which are funded under various paratransit programs.
– Review video to investigate criminal acts involving taxi drivers or riders.

Surveillance Oversight Review Dates

COIT Review: April 21, 2022
Board of Supervisors Review: TBD

– Review video data to investigate accidents involving a taxi cab.

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Technology Details

The following is a product description of Taxi Dashboard Cameras:

Of the many manufacturers taxi cab companies and other taxi permittees may choose from, Janus is the most commonly used. Janus Cam V1 HD offers a 120-degree lens with a wide range of vision, enabling drivers to capture events as wide as the street on which they travel as well as within the vehicle itself. The Janus V1 HD captures video in a number of resolutions, and backup capabilities allow images to be stored in JPEG, AVI, JDR, BMP and G-SENSOR. The Janus V1 HD is the perfect in-vehicle security camera for trucks, police cars, taxis, ambulances and other emergency vehicles, as well as, personal vehicles. Every Janus Cam comes with an easy to use, out-of-the-box software. Easily manage your event time stamps and categorize your clips. The software also comes with a built-in speedometer and a g-sensor graph.

A. How the Taxi Dashboard Camera Works.

To function, Taxi Dashboard Cameras consist of one camera device with two lenses. The camera device is typically mounted behind the rearview mirror or in the upper portion of the windshield of the passenger side of the taxi cab and captures images in the cabin and on the road in front of the taxi cab. Video is saved to secure digital (SD) cards.

. The Department does not own the Dashboard Cameras inside the taxicab and has no control over how the data outside of department custody is handled or stored.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of video data from the Taxi Dashboard Camera has the following benefits for the residents of the City and County of San Francisco:

- X Accessibility: Ensures consumer protection and public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders. Allows video audits of accessible trips subsidized by public funds
- X Criminal Justice: Ensures consumer protection and public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders or drivers, while also serving as a deterrent by recording incidents in the taxi cab. .
- X Health: Ensures consumer protection and public health by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders.
- X Public Safety: Ensures public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders, as well as serving as a deterrent to drivers who may otherwise operate a vehicle in an unsafe manner.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

- Dignity Loss (e.g., embarrassment and emotional distress). Taxi cab drivers and riders may experience dignity loss if the surveillance technology records videos of them committing acts or experiencing situations that are embarrassing or distressing for them (e.g., altercations between drivers and riders, criminal acts) and those videos are released to the public.
    - technical measures make this impact minimal because taxi cab companies store video files on secure digital (SD) cards, which are password protected and require proprietary software to view. This prevents unauthorized access to video; these images are only accessed when required under an authorized business case and are generally not available to the public.
    - Administrative safeguards make this impact minimal because only designated Department staff have access to view video files, which occurs only under an authorized business case. SD cards are returned to the respective taxi cab company once Department review is complete, unless the video file becomes the subject of an appeal, an accident investigation or criminal investigation. Video files retained by the Department are generally not available to the public.

    - Physical protections make this impact minimal because SD cards while in Department custody are stored by authorized Department staff in a secure office setting that is not open to the public.
- Discrimination (i.e., unfair or unethical differential treatment of individuals or denial of civil rights). Taxi cab drivers and riders may experience discrimination if the surveillance technology records their images based on their belonging to a specific group (e.g., based on color, race, or ethnicity).
    - technical measures make this impact unlikely because the technology is deployed equally on all taxi cabs regulated by the City
    - Administrative safeguards make this unlikely because Department staff will request videos from the taxi cab companies only under an authorized use case and not based on the Department's assessment of the video.
- Economic Loss (e.g., identify theft/misidentification). Taxi cab drivers and riders may experience economic loss if their identities are stolen through unauthorized access to data collected by the surveillance technology.
    - technical measures make this impact unlikely because the surveillance technology does not record personally identifiable information from taxi company drivers or riders that is typically used for identity theft (e.g., names, addresses, credit card numbers, social security numbers, etc.).
- Loss of Autonomy (e.g., loss of control over decisions on how personal information is used or processed). Taxi cab drivers and riders may experience loss of autonomy if video recordings of their likeness are used for purposes other than authorized use cases or made generally available to the public.
    - Administrative safeguards make this impact minimal because only designated Department staff have access to view video files, which occurs only under an authorized business case. SD cards are returned to the respective taxi cab company once Department review is complete, unless the video file becomes the subject of an appeal, an accident investigation or criminal investigation. Video files retained by the Department are generally not available to the public.
    - Physical protections make this impact minimal because SD cards while in Department custody are stored in the possession of authorized Department staff in a secure office setting that is not open to the public.
- Loss of Liberty (i.e., improper exposure to arrest or detainment due to incomplete or inaccurate data). Taxi cab drivers and riders may experience loss of liberty if law enforcement misidentifies them in connection with a crime recorded by the surveillance technology.
    - Administrative safeguards make this impact unlikely because law enforcement verify the identities of taxi cab drivers and riders using data from other sources (e.g., taxi cab company records and credit card transactions) before they take action.

- Physical Harm (e.g., physical harm or death). Taxi cab drivers and riders may experience physical if they are identified, tracked, and physically attacked based on data collected by the surveillance technology.
    - technical measures make this impact unlikely because the surveillance technology does not record personally identifiable information from taxi company drivers or riders that (other than law enforcement) could reasonably be used to identity individuals (e.g., names, addresses, credit card numbers, social security numbers, etc.).
    - Administrative safeguards make this impact minimal because only designated Department staff have access to view video files, which occurs only under an authorized business case. SD cards are returned to the respective taxi cab company once Department review is complete, unless the video file becomes the subject of an appeal, an accident investigation or criminal investigation. Video files retained by the Department are generally not available to the public.
    - Physical protections make this impact minimal because SD cards while in Department custody are stored by authorized Department staff in a secure office setting in a secure office setting that is not open to the public.
- Loss of Trust (e.g., breach of implicit or explicit expectations or agreements about the processing of data, or failure to meet subjects' expectation of privacy for information collected). Taxi cab drivers and riders may experience loss of autonomy if video recordings of their likeness are used for purposed other than authorized use cases or made generally available to the public.
    - Administrative safeguards make this impact minimal because only designated Department staff have access to view video files, which occurs only under an authorized business case. SD cards are returned to the respective taxi cab company once Department review is complete, unless the video file becomes the subject of an appeal, an accident investigation or criminal investigation. Video files retained by the Department are generally not available to the public.
    - Physical protections make this impact minimal because SD cards while in Department custody are stored by authorized Department staff in a secure office setting that is not open to the public.
- Overall
    - Administrative Safeguards: The Department provides access to video data received from the taxi cab companies and other taxi permittees only to authorized staff, as required to perform the use cases. All access to videos is password protected and each taxi cab company has a separate password.
    - Technical Safeguards: The Department does not have continuous or instant access to video data or information recorded by the technology. The Department must request video data or information for specific incidents after they occur and the taxi cab company provides video files on password secure digital (SD) cards.

- Physical Safeguards: Password protected secure digital (SD) cards are kept in the custody of only authorized Department staff.

C. Fiscal Analysis of Costs and Benefits

The Department's use of limited video data from Taxi Dashboard Cameras yields the following business and operations benefits:

- X Allows investigations to proceed: The Department is responsible for managing surface transportation in the City. The Department uses video data and information from the technology to ensure taxi cab companies and other taxi permittees and drivers comply with applicable requirements and conditions under Article 1100 (Regulation of Motor Vehicles to Hire) of Division II of the Transp. , which helps ensure consumer protection and, public health and safety.
- X Improved Data Quality: the alternative is conducting witness interviews after receiving a report or complaint. Having a recording of an incident helps to inform whether corrective action is warranted.
- X Time Savings: The alternative is relying solely on witness interviews, which can be time consuming and may not be reliable in some cases.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): 0. The Department does not own or have staff that support the use of the surveillance technology because it does not own this technology. Taxi cab companies and other taxi permittees and their drivers support the technology.
- The Department does not fund its use and maintenance of the surveillance technology. The taxi cab companies and other taxi permittees and their drivers pay for the surveillance technology.

COMPARISON TO OTHER JURISDICTIONS

Taxi Dashboard Cameras are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Taxi Dashboard Camera
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 video data from the Taxi Dashboard Camera 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 San Francisco Municipal Transportation Agency's ("SFMTA", "Municipal Transportation Agency", or "Department") mission is to connect San Francisco through a safe, equitable, and sustainable transportation system.

The Surveillance Technology Policy ("Policy") defines the manner in which the video data from the Taxi Dashboard Camera 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 video data from the Taxi Dashboard Camera, 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 the video data from the Taxi Dashboard Camera technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– Review recording of on-board incidents based upon complaints received from the public and at appeals hearing in response to a fine, suspension or response to fine revocation.
– Review video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transportation Code.
– Review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides. For example, under its wheelchair program taxi incentive, the Department reviews video data from the technology to confirm that taxi cab drivers pick up individuals with certain disabilities before paying drivers for those rides, which are funded under various paratransit programs.
– Review video to investigate criminal acts involving taxi drivers or riders.

– Review video data to investigate accidents involving a taxi cab.

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. Additionally, department may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Video data from the Taxi Dashboard Camera supports the Department's mission and provides important operational value in the following ways:

Taxis are one of several modes of transportation the Department regulates within the City. Taxi cab companies and other taxi permittees that operate in the City are subject to a number of requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transp. Code to ensure safety, equity of service, and sustainability among other goals. The City uses video data or information it acquires from the taxi cab companies and other taxi permittees' use of the technology to enforce their compliance with these requirements and conditions.

In addition, video data from the Taxi Dashboard Camera promises to benefit residents in the following ways:

- Accessibility: Ensures consumer protection and public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders. Allows video audits of accessible trips subsidized by public funds
- Criminal Justice: Ensures consumer protection and public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders or drivers, while also serving as a deterrent by recording incidents in the taxi cab.
- Health: Ensures consumer protection and public health by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders.
- Public Safety: Ensures public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders, as well as serving as a deterrent to drivers who may otherwise operate a vehicle in an unsafe manner.

Video data from the Taxi Dashboard Camera will benefit the department in the following ways:

- Allows investigations to proceed: The Department is responsible for managing surface transportation in the City. The Department uses video data and information from the technology to ensure taxicab companies and other taxi permittees and drivers comply with applicable requirements and conditions under Article 1100 (Regulation of Motor Vehicles to Hire) of Division II of the Transp., which helps ensure consumer protection and, public health and safety.
- Improved Data Quality: the alternative is conducting witness interviews after receiving a report or complaint. Having a recording of an incident helps to inform whether corrective action is warranted.
- Time Savings: The alternative is relying solely on witness interviews, which can be time consuming and may not be reliable in some cases.

To achieve its intended purpose, the video data acquired from the Taxi Dashboard Camera (hereinafter referred to as "surveillance technology") consists of one camera device with two lenses. The camera device is typically mounted behind the rearview mirror or in the upper portion of the windshield of the passenger side of the taxi cab and captures images in the cabin and on the road in front of the taxi cab. Video is saved to secure digital (SD) cards.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Department shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- Video and audio recordings from taxi cab cabins, including conversations between riders with cab drivers. Front facing video cameras record traffic conditions on the road and routes taken. All information is Level 3 sensitivity per the City's Data Classification Standard.

Notification: Department does not own dashboard cameras in taxi cabs and therefore does not provide public notice. The Transportation Code requires that taxis have a notice notifying passengers of the presence of a security camera in the vehicle.

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Video is viewable on proprietary software (mainly Janus) and is password protected.

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:

9174 Enforcement and Legal Affairs Manager

9177 Investigations Supervisor

8167 Administrative Hearing Examiner

9183 Taxi Director

9144 Taxi Investigators (8 personnel)

B. Members of the public, including criminal defendants

The Municipal Transportation Agency 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Department shall, at minimum, apply the following safeguards:

Video data are not accessible to unauthorized parties. (All access is password protected.)

Data Sharing: The Municipal Transportation Agency will endeavor to ensure that other agencies or departments that receive data collected from a Taxi Cab Dashboard Camera 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.

The Municipal Transportation Agency 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)

The Municipal Transportation Agency Department shall ensure all PII and restricted data is adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

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 response.

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.

- 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.

The Municipal Transportation Agency 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 currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Type	**Recipient**
Video (recording on secure digital (SD) card or possible copy from the cloud.)	SFMTA, San Francisco Police Department (SFPD), District Attorney and Public Defender

Data sharing occurs at the following frequency:

The Department shares data from the technology upon request and in accordance with the authorized use cases. The frequency of sharing varies with the timing and number of incidents that trigger requests..

B. External Data Sharing

Department shares the following data with the recipients:

Type	**Recipient**
Department shares video it receives from taxi cab companies and other taxi permittees with outside entities using secure digital SD cards.	California Highway Patrol (CHP) and other law enforcement agencies but only with a warrant

Data sharing occurs at the following frequency:

Varies. Depends on request.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy the Department will endeavor to ensure that other agencies or departments with which it shares data from the technology receive a copy of and comply with the policy. The Department will

ensure administrative, technical, and physical safeguards are in place before sharing data internally with other City departments. 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.
- Evaluate what data can be permissibly shared with members of the public should a request be made in accordance with San Francisco's Sunshine Ordinance.
- Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	**Retention Justification**
For data used at taxi disciplinary hearings, data is retained indefinitely. For data used for other purposes, including compliance related audits, SD cards are returned to the taxi cab companies and other taxi permittees after audit is performed.	Pursuant to the Department retention policy, video relating to an appeal are stored as part of the hearing file. Video for any other purpose is not retained and is returned to the taxi cab company at the completion of the investigation or audit.

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.

Department must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- Local Storage

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- For data used at taxi disciplinary hearings, data is retained indefinitely. For data used for other purposes, including compliance related audits,

SD cards are returned to the taxi cab companies and other taxi permittees after audit is performed.

Processes and Applications:

- The Department does not have or require any process or application to scrub images of individual taxi cab drivers or riders (which are the personal identifiable information typically recorded by the technology) because the Department requires these images to perform authorized use cases.

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.

At the very least, 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. 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. This part of the policy does not apply as the Department does not have a training policy.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Department will assign personnel to oversee and enforce compliance with the policy .

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

- 9174 Enforcement and Legal Affairs Manager.

Sanctions for violations of this Policy include the following:

- Violations of the Policy may result in disciplinary action or sanctions commensurate with the severity of the violation. Sanctions may include written warning, suspension, or 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 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:

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. To do so, Department shall:

The Department will respond to complaints submitted through 311 within the time line specified in the Department's 311 response policy.

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.

Surveillance Impact Report

War Memorial
SF Symphony Security Cameras

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco War Memorial & Performing Arts Center manages, maintains and operates safe, accessible, world-class venues to promote cultural, educational, and entertainment opportunities in a cost-effective manner for enjoyment by the public, while best serving the purposes and beneficiaries of the War Memorial Trust.

This impact assessment applies to security camera data sharing between War Memorial and the following entities:

- San Francisco Symphony

In line with its mission, the Department shall use San Francisco Symphony security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Reviewing camera footage provided by SF Symphony upon request in the event of an incident.

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

Further, processing of personal data revealing 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.

Department technology may be deployed in the following locations, based on use case:

SF Symphony Security Cameras are located in public and office/work areas of Davies Symphony Hall and associated grounds.

Surveillance Oversight Review Dates
COIT Review: April 21, 2022
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

Cameras: AXIS, MODELS P3327-LV, P3227-LVE, P3807-PVE
Server: EXACQVISION IP04-30T-R2A 30-TB NVR
Software: EXAQ EVIP-01 PROFESSIONAL
Vendor: G4S

A. How It Works

To function, SF Symphony Security cameras primary functions are to provide live views and record video footage to a dedicated, secure server. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a limited amount of time.

All data collected or processed by SF Symphony Security Cameras will be handled or stored by, SF Symphony, an outside provider or third-party vendor on an ongoing basis.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of security cameras has the following benefits for the residents of the City and County of San Francisco:

☐	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.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

War Memorial believes Tenant/Contractor security cameras pose potential risks to civil liberties in respect to dignity loss and loss of liberty.

An individual could be embarrassed or experience emotional distress if cameras capture behaviors, appearances, or circumstances by which they might feel humiliated. Examples include views of someone exhibiting an emotional outburst, a person's clothing or hair being disheveled, or someone having their physique ridiculed or leered at. Risks for loss of dignity are reduced by restricting access to live views, as well as any recorded footage shared with Department by Tenant/Contractor, to a limited number of trained Security staff. In addition, live camera views provided to Department staff do not pan, tilt or zoom, thus removing possible temptation for system operators to use those features to follow or enhance views of individuals. Audio is also not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing like clothing worn by someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and any recorded footage shared with Department by Tenant/Contractor to a limited number of trained personnel.

C. Fiscal Analysis of Costs and Benefits

The Department's use of surveillance cameras yields the following business and operations benefits

Benefit		**Description**
X	Financial Savings	San Francisco Symphony Security Camera Systems will save on building or patrol officers. Equipment is owned and operated by non-city entity.
X	Time Savings	SF Symphony's Security Camera Systems will run 24/7, thus decreasing or 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.

Number of FTE (new & existing)	0	
Classification	N/A	
	Annual Cost	***One-Time Cost***
Software	***0***	0
Hardware/Equipment	*0*	0
Professional Services	*0*	0
Training	*0*	*0*
Other	0	0
Total Cost	***0***	*0*

No cost to Department. SF Symphony owns, operates and maintains the security camera system and associated equipment.

COMPARISON TO OTHER JURISDICTIONS

Surveillance Camera Technologies like the SF Symphony Security Camera System are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Mapped Crime Statistics

The general location(s) it may be deployed and crime statistics for any location(s):

SF Symphony security cameras are located in public and office/work areas of Davies Symphony Hall and associated grounds.

Crime statistics for SFPD Northern Station region are attached and can be found online here:
https://www.sanfranciscopolice.org/sites/default/files/2021-12/SFPDCompstatOctober2021-20211207.pdf
or
https://www.sanfranciscopolice.org/stay-safe/crime-data/crime-reports

Surveillance Technology Policy

Tenant/Contractor Security Cameras
War Memorial

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 San Francisco Symphony ("Tenant/Contractor") Security Camera System by San Francisco War Memorial & Performing Arts Center ("War Memorial Department", "War Memorial", or "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 San Francisco War Memorial & Performing Arts Center manages, maintains and operates safe, accessible, world-class venues to promote cultural, educational, and entertainment opportunities in a cost-effective manner for enjoyment by the public, while best serving the purposes and beneficiaries of the War Memorial Trust.

The Surveillance Technology Policy ("Policy") defines the manner in which the Tenant/Contractor 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

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

- San Francisco Symphony

City departments are limited in their use of security camera equipment and footage that is owned and operated by non-City entities to the following authorized use cases and requirements listed in this Policy only.

Authorized Use(s):

1. Live monitoring internal office space and public area of Davies Symphony Hall.
2. Reviewing camera footage provided by Tenant/Contractor upon request 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

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

Cameras: AXIS, MODELS P3327-LV, P3227-LVE, P3807-PVE
Server: EXACQVISION IP04-30T-R2A 30-TB NVR
Software: EXAQ EVIP-01 PROFESSIONAL
Vendor: G4S
Location: SF Symphony surveillance cameras are located in public and office/work areas of Davies Symphony Hall and associated grounds.

Security Cameras will benefit the department in the following ways:

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
X	Criminal Justice	Review video footage after a security incident.
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. Equipment is owned and operated by non-city entity.
X	Time Savings	Tenant/Contractor Security Camera Systems run 24/7, thus decreasing or eliminating building or patrol officer supervision.
X	Staff Safety	Tenant/Contractor Security cameras help identify violations of 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	Service Levels	Tenant/Contractor Security cameras will enhance effectiveness of incident response and result in an 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 receive data that is 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

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.

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.

- 8207 - Building and Grounds Patrol Officers,
- 8211 - Supervisor Building and Grounds Patrol Officer,
- 0922 - Director of Security,
- 1093 - IT Manager,
- 1844 - Facilities Administrator
- 0962 - Managing Director
- 0952 - Assistant Managing Director

The following providers are required to support and maintain the surveillance technology and its associated data to ensure it remains functional:

- GS4, Tenant/Contractor's support vendor

B. Members of the public

Data collected by surveillance technology will not be made generally available to members of the public.

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.

Data Security:	Department shall secure any PII received from Tenant/Contractor (or shared by Tenant/Contractor) 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/Contractor 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 by the Department 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 for/intended use of data, department requesting data (if any), date/time of data access, outcome of data processing, as well as date the 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 at its sole discretion. The Department will endeavor to ensure that other agencies or departments that may receive data collected under War Memorial's Tenant/Contractor Security Camera Policy will act in conformity with this Surveillance Technology Policy. Data is shared by Tenant/Contractor with the Department on the following schedule: ✓ As needed *A. Internal Data Sharing* Department does not share Tenant/Contractor Security camera data with internal or external recipients. *B. External Data Sharing:* Department does not share Tenant/Contractor Security camera data with internal or external recipients.
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. 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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s): - Security Camera data shared with Department by Tenant/Contractor will be stored only for the period necessary for investigation or litigation following an incident.

	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:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Practices: - Data is disposed following the period that it is relevant to an ongoing investigation or litigation. Processes and Applications: - Delete/reformat, wipe, overwrite of existing data, or degaussing.
Contracts and/or Legal Agreements:	The War Memorial Department does not have a contract or legal agreement with a third-party entity governing third-party data use, including but not limited to third party data use, sharing, signage, retention, and/or disposal.
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 per COIT policy. - Prior to accessing or using data, authorized individuals within the Department receive instruction regarding authorized and prohibited uses.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

- On a monthly basis, retained Tenant/Contractor footage or images shall be reviewed to determine its continued relevance for any ongoing investigations or litigation.

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

- 0922, Director of Security
- 8211, Supervisor Building and Grounds Patrol Officer
- 1844, Facilities Administrator

Sanctions for violations of this Policy include the following:

- 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

Third-Party or Tenant/Contractor	Non-City Entity that owns and operates security cameras and shares security camera footage with a City department.
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."

QUESTIONS & CONCERNS

Public:

Complaints or concerns can be submitted to the Department by sending an email to WarMemorialinfo@sfgov.org.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall monitor the War Memorial information email box throughout the day during standard business hours. Any communications to that email address are responded to directly or brought to the attention of responsible staff.

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.

City & County of San Francisco
London N. Breed, Mayor

Office of the City Administrator
Carmen Chu, City Administrator
Jillian Johnson, Director
Committee on Information Technology

To: Angela Calvillo
Clerk of Board of Supervisors

From: Carmen Chu, City Administrator
Jillian Johnson, Director, Committee of Information Technology

Date: July 18, 2022

Subject: Legislation introduced for Approval of Surveillance Technology Policies for Multiple City Departments

---

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit Surveillance Technology Policies and Impact Reports for the following technologies to the Board of Supervisors for their review:

- Automatic License Plate Readers (ALPR)
- Biometric Processing Software and/or System
- Body-Worn Cameras
- People-Counting Camera
- Security Cameras
- Third-Party Security Cameras
- Location Management System
- Computer Management System
- Social Media Monitoring Software

The Committee on Information Technology (COIT) and its subcommittee, the Privacy and Surveillance Advisory Board (PSAB), held public meetings over the course of the last year to engage the public in developing these Surveillance Technology policies. All details of these discussions are available at sf.gov/COIT.

The following sections provide more detail on the departments seeking Board of Supervisors approval for their surveillance technology policies, and the COIT recommended course of action.

If you have questions on the review process, please direct questions to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Automatic License Plate Readers (ALPR)

Department	Authorized Uses
Municipal Transportation Agency (MTA)	1. Enforce parking restrictions and laws. 2. Transit Only Lane Enforcement (TOLE). 3. Link individual vehicles to their times of entry/exit into City-owned parking garages and lots to accurately calculate parking fees. 4. Identify vehicles that are the subject of an active investigation by the SFPD (e.g., vehicles included on "hot lists" generated by the SFPD –see Appendix B & C of MTA policy, and page 8 of SFPD ALPR Policy). 5. Analysis of and reporting on parking and curb usage.

ALPR Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
September 24, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the ALPR Surveillance Technology Policy for the MTA.

Biometric Processing Software or System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on continuous alcohol monitoring (CAM) in San Francisco with a court order. The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing. CAM data is analyzed on a daily basis by probation officers to ensure compliance with the Court's order.

Biometric Processing Software/System Public Meeting Dates:

Date	Meeting
January 14, 2022	Privacy and Surveillance Advisory Board (PSAB)
February 17, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Biometric Processing System Surveillance Technology Policy for Juvenile Probation.

Body-Worn Cameras

Departments	Authorized Uses
Fire	- Use by Public Information Officer (PIO) at large incidents to capture video of surroundings and the totality of the incident
Recreation and Parks	- Recording video and audio footage in the event of an incident. Incidents can be: o Actual or potential criminal conduct o Situation when a Park Ranger reasonably believes recordings of evidentiary value may be obtained o Calls for service involving a crime where the recording may aid in the apprehension/ prosecution of a suspect - Providing recording to law enforcement or other authorized persons upon request.

Body-Worn Cameras Public Meeting Dates:

Date	Meeting	Departments
September 10, 2021	PSAB	Fire
September 24, 2021	PSAB	Recreation and Parks
October 21, 2021	COIT	Fire, Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Body-Worn Camera Surveillance Technology Policies for the Fire Department and the Recreation and Parks Department.

People-Counting Cameras

Departments	Authorized Uses
Library	- To tally the entry and exit of Library visitors at all 28 public facilities. - To track usage of meeting rooms, elevators and restrooms for purposes of resource allocation.

People-Counting Cameras Public Meeting Dates:

Date	Meeting
January 28, 2022	Privacy and Surveillance Advisory Board (PSAB)
March 11, 2022	Privacy and Surveillance Advisory Board (PSAB)
April 21, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the People-Counting Camera Surveillance Technology policy for the Library.

Security Cameras

Departments	Authorized Uses
Elections	- Live monitoring of voting center lines. - Live monitoring of Department staff during elections operations. - Recording of video and images of Department staff during elections operations. - Reviewing camera footage of Department staff in the event of an incident. - Sharing camera footage of Department staff with the public to promote transparency into elections operations.

Security Cameras Public Meeting Dates:

Date	Meeting
October 22, 2021	Privacy and Surveillance Advisory Board (PSAB)
November 18, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Security Camera Surveillance Technology Policy for the Department of Elections.

Third-Party Security Cameras

Departments	Authorized Uses
Airport (AIR)	- Reviewing camera footage in the event of an incident. - Approving Tenant's disclosure of digital recordings and other data from its security camera system.
Municipal Transportation Agency (MTA)	- Review recording of on-board incidents based upon complaints received from the public and at appeals hearing in response to a fine, suspension or response to fine revocation. - Review video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transportation Code. - Review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides. For example, under its wheelchair program taxi incentive, the Department reviews video data from the technology to confirm that taxi cab drivers pick up individuals with certain disabilities before paying drivers for those rides, which are funded under various paratransit programs. - Review video to investigate criminal acts involving taxi drivers or riders. - Review video data to investigate accidents involving a taxi cab.
War Memorial (WAR)	- Live monitoring internal office space and public area of Davies Symphony Hall. - Reviewing camera footage provided by Tenant/Contractor upon request in the event of an incident.

Third-Party Security Cameras Public Meeting Dates:

Date	Meeting	Departments
October 22, 2021	PSAB	WAR
January 14, 2022	PSAB	WAR, AIR
January 28, 2022	PSAB	AIR
February 17, 2022	COIT	AIR
March 11, 2022	PSAB	MTA
April 21, 2022	COIT	WAR, MTA

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Third-Party Security Camera Surveillance Technology Policies for the Airport, Municipal Transportation Agency, and War Memorial.

Location Management System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on electronic monitoring in San Francisco with a court order. The Court may order a youth to be placed on electronic monitoring as an alternative to detention. - Electronic monitoring (EM) may also be added as a condition of probation if additional supervision is warranted. EM data is analyzed on a daily basis by probation officers to ensure compliance with: - Court ordered curfews o Inclusion zones: addresses/areas where the minor has approval to be present, for example their home, school, work. o Exclusion zones: addresses/areas where the minor should not be present, including Stay Away orders o Schedules: To monitor school attendance, program participation, work.
Recreation and Parks	- Confirm that the person who reserved the booking for a tennis court is at the location at the reserved time. - Utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time.

Location Management System Public Meeting Dates:

Date	Meeting	Department
October 22, 2021	PSAB	Juvenile Probation
November 18, 2021	COIT	Juvenile Probation
March 11, 2022	PSAB	Recreation and Parks
May 27, 2022	PSAB	Recreation and Parks
June 16, 2022	COIT	Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Location Management Surveillance Technology Policies for Juvenile Probation and the Recreation and Parks Department.

Social Media Monitoring Software

Department	Authorized Uses
Library	- Plan and execute more effective and strategic campaigns across social media platforms. - Schedule multiple social media posts in advance. - Create and monitor multiple streams of content across various platforms. - Maintain active social media presence that is automated, specifically on weekends when staff is off. - Ensure consistency of messaging across all social media platforms. - Track post performance and analyze trends to improve content and strategy. - Create reports.

Social Media Monitoring Software Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Social Media Monitoring Software Surveillance Technology Policy for the Library.

Computer Management System

Departments	Authorized Uses
Library	- The authorized use case for the TBS Computer Time and Print Management tool is to provide time-delimited public access to library computers and allow the public to print, copy, scan and fax documents, as well as track usage of computers and print resources throughout the library's 28 facilities for purposes of resource allocation and management.The five specific components within TBS Computer Time and Print Management are as follows: • MyPC: Manages patron access to library computers and regulates amount of time each patron can use computers • EZ Booking: Allows patrons to manage their reservations in MyPC, schedule public computer use, etc. • Papercut/EPrintIt: Manages public print jobs sent from library computers and patrons' personal devices, allowing them to print their documents on library printers. Also allows select library staff members, in the interest of customer service and support, to retrieve and print jobs submitted to the system by users during the 24-hour period in which documents are retrievable. This allows staff to print jobs when printers fail, when print jobs do not meet user expectations, to intermediate when users are struggling with technology, etc. • Allows library patrons to scan, manipulate, manage, print, email, fax and save documents using either the library's flat-bed or document feeder scanners. • Payment Kiosk: Allows patrons to pay for print and copy jobs processed through Papercut/EPrintIt and/or ScanEZ.

Security Cameras Public Meeting Dates:

Date	Meeting
May 27, 2022	Privacy and Surveillance Advisory Board (PSAB)

June 16, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Computer Management System Surveillance Technology Policy for the Library.

BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

M E M O R A N D U M

TO: Jeffrey Tumlin, Executive Director, Municipal Transportation Agency
Katherine Miller, Chief Probation Officer, Juvenile Probation Dept.
Jeanine Nicholson, Chief, Fire Department
Phil Ginsburg, General Manager, Recreation and Parks Dept.
Michael Lambert, City Librarian, Library Department
John Arntz, Director, Department of Elections
Ivar C. Satero, Director, Airport Dept.
Chief William Scott, Police Dept.
Elizabeth Murray, Director, War Memorial

FROM: Victor Young, Assistant Clerk

DATE: August 4, 20222

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed legislation:

File No. 220843 Administrative Code - Approval of Surveillance Technology Policies for Multiple City Departments

Ordinance approving Surveillance Technology Policies governing the use of 1) Automatic License Plate Readers by the Municipal Transportation Agency, 2) Biometric Processing Software or System by the Juvenile Probation Department, 3) Body-Worn Cameras by the Fire Department and Recreation and Park Department, 4) People-Counting Camera by the Library, 5) Security Cameras by the Department of Elections, 6) Third-Party Security Cameras by the Airport, Municipal Transportation Agency, Police Department, and War Memorial, 7) Location Management Systems by the Juvenile Probation Department and the Recreation and Park Department, 8) Computer Management System by the Library, and 9) Social Media Monitoring Software by the Library; and making required findings in support of said approvals.

If you have comments or reports to be included with the file, please forward them to me at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

cc: Kate Breen, SFMTA
Janet Martinsen, SFMTA
Joel Ramos, SFMTA
Christine Silva, SFMTA

Sheryl Cowan, Juvenile Probation
Theresa Ludwig, Fire Department
Sarah Madland, Recreation and Park
Ashley Summers, Recreation and Park
Almer Castillo, Library
Cathey Widener, Airport Dept.
Corina Monzon, Airport Commission
Lisa Ortiz, Police Dept.
Lili Gamero, Police Dept.
Diana Oliva-Aroche, Police Dept.
Sgt. Stacy Youngblood, Police Commission
Jennifer Norris, War Memorial