Surveillance Technology Policy

Security Cameras with CCTV software
Animal Care & Control

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 Security Cameras with CCTV 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 Department's mission is:

The San Francisco Department of Animal Care & Control (SFACC) is a taxpayer-funded, open-admission animal shelter. Since 1989, SFACC has provided housing, care, and medical treatment to wild, exotic and domestic stray, lost, abandoned, sick, injured, and surrendered animals. SFACC's doors are open to all animals in need regardless of species, medical, or behavioral condition. The shelter also enforces all state and local Animal Control and Welfare laws and is the first responder for animals in natural disasters and citizen emergencies. SFACC shelters homeless, neglected, and abused animals and offers a variety of services to the community. SFACC is the local City agency that investigates animal cruelty, abuse or neglect, enforces animal welfare laws, rescues wildlife and wild birds in distress, and aids domestic animals in need. SFACC aims to adopt, rehome, or reunite domestic animals with their guardians and release wildlife to their native habitat.

The Surveillance Technology Policy ("Policy") defines the manner in which the surveillance technology 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 the surveillance technology 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 Security Cameras with CCTV 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):

– *Live video monitoring feeds.*
– *Recording of videos and images.*

Surveillance Oversight Review Dates
PSAB Review: Recommended with changes 1/27/2023
COIT Review: 2/16/2023
Board of Supervisors Approval: TBD

– *Reviewing camera footage in the event of an incident, both in real time and later for debriefing.*
– *Providing footage or images to law enforcement or other authorized persons following an incident or upon request.*
– *To monitor building performance.*

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

Reason for Technology Use

The surveillance technology supports the Department's mission and provides important operational value in the following ways:

The technology ensures that all animals housed on-premises are safe from theft, cruelty, abuse, or neglect while in care. Additionally, it aids with internal incident investigations, allegations of mistreatment on-site, and crimes against the organization. The cameras are also used to protect the facility against vandalism

Description of Technology

The cameras are motion activated and record events. A few Cameras in critical operational areas record full frame video. There are two locations (with highly visible posted signage) that also record audio (intake lobby, public hearing room) because of the potential, and demonstrated, emotional volatility of interactions in these locations.

Resident Benefits

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

Benefit	Description
▪ Education	
▪ Community Development	
▪ Health	
▪ Environment	

X	Criminal Justice	Video footage allows us to document graffiti and other damage to the building and refer that to San Francisco Police Department for possible prosecution. Additionally, there have been instances of violent behavior and animal cruelty on premises that warrant investigation and immediate action.
▪	Jobs	
▪	Housing	
X	Other: Public Safety, Animal Welfare	We have had to evacuate the building when a member of the public broke in through a locked door. We were able to safely escort members of the public out through the back of the building and away from the threat because we were able to use the cameras to determine that the only problem was at the front of the building. The cameras also allowed people still in the building to be alerted to the arrival of the police and the end to the threat. We house 100-250 animals per day with 50 staff and 150 volunteers. The cameras help us review reported incidents so that we can determine if our standards of care were violated. Recently, reviewing footage enabled us to determine that a volunteer was violating our code of conduct in regards to proper dog handling. We were also able to review footage to determine how a dog escaped its enclosure which led to a dog fight. Our animal population is vulnerable and cannot tell us in words if there's a problem. They depend on us to be vigilant and investigate problems.

Department Benefits

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

	Benefit	Description
▪	Financial Savings	
▪	Time Savings	
X	Staff Safety	Our cameras are critical to staff safety. It is common for people trying to claim, look for, or surrender animals to become quite emotional, even violent. This is particularly true for people whose animals are being held as part of an investigation or for enforcement of the pit bull spay/neuter

		ordinance. The cameras allow us to see what happened just before the confrontation started and establish whether there are other possible participants who are not in immediate view. This all helps us determine whether we need to call for police assistance. When police do arrive, the footage helps confirm what happened.

- Data Quality

X	Other: Animal Welfare	We house 100-250 animals per day with 50 staff and 150 volunteers. The cameras help us review reported incidents so that we can determine if our standards of care were violated. Recently, reviewing footage enabled us to determine that a volunteer was violating our code of conduct in regards to proper dog handling. We were also able to review footage to determine how a dog escaped its enclosure which led to a dog fight. Our animal population is vulnerable and cannot tell us in words if there's a problem. They depend on us to be vigilant and investigate problems

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.

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

The surveillance technology collects some or all of the following data type(s):

Data Type(s)	*Format(s)*	*Classification*
Video Images	.AVE	Level 1-2
Audio	.AVE	Level 1-2

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. The notification signage are located at all public entrances, at the main gate of the shelter parking lot, and next to the employee entrance at the back of the building. 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:

X Information on the surveillance technology
X Description of the authorized use
X Type of data collected
- Data retention
- Department identification
X Contact information

Access: All parties requesting access must adhere to the following rules and processes:

- Select employees (the Director, Deputy Director, Operations Manager, Principal Analyst, Animal Control Supervisor (Field Services Captain) and the Field Services Assistant Supervisor(s)) may view recorded data based on the authorized use cases. These accounts are password-protected and set-up off site by Media Services.

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:

- Director – 0962
- Deputy Director – 0952
- Operations Manager – 0923
- Principal Administrative Analyst – 1824
- Animal Control Supervisor – 3379
- Field Services Assistant Supervisors – 3378

All other employees on premises may view live incidental footage via security monitors located in specific staff-only areas of the shelter.

- 1452 - Executive Secretary, 1
- 9920 - Public Service Aide, 3

- 2292 - Shelter Veterinarian, 2
- 3375 - Animal Health Technician, 2
- 3371 - Animal Care Supervisor, 1
- 3376 - Assistant Animal Care Supervisor, 2
- 3370 - Animal Care Attendants, 17
- 3374 - Volunteer & Outreach Coordinator, 1
- 1310 - Public Relations Assistant, 2
- 1435 - Shelter Office Supervisor, 1
- 1424 - Clerk Typist, 1
- 1434 - Shelter Service Representative, 9
- 3372 - Animal Control Officer, 12

B. Members of the public

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

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.

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

Department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses dictated by this policy. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

More specifically, Department training will include:

To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures. Department staff also participate in annual cybersecurity training.

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.

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

All data is password protected. No employee on premises, including select authorized users (Director, Deputy Director, Operations Manager, Principal Administrative Analyst, Field Services Captain, or Field Services Assistant Supervisors) has the ability to edit, download, or export recorded data. Department of Real Estate (RED) Media Security Systems Division maintains the computer storage, and will only export video to authorized Animal Care and Control staff after documented receipt of written and approved request.

Data Storage: Data will be stored in the following location:

X Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)

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

Data Sharing: Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology will act in conformity with this Policy.

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 shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. *(See Data Security)*

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their legal obligations.

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

- Confirm the purpose of the data sharing aligns with the department's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

A. Internal Data Sharing:

The department shares the following data with recipients within the City and County of San Francisco:

Data Type	Data Recipient
Video and audio	Real Estate Department: San Francisco Police Department ("SFPD") (on request when approved for release by Real Estate Department Surveillance Policy or Animal Care and Control Surveillance Policy, if ongoing law

	enforcement incident or when approved for release with a SFPD case number.) Animal Care and Control: Will request an exported file from RED using standard process. SFACC will then provide this file to SFPD for investigation and request a case number for recordkeeping.

Frequency - Data sharing occurs at the following frequency:
As Manager of Record for stored data, Real Estate Department has total access. SFPD receives data on an as needed basis during ongoing security threats or upon request if a crime is committed.

B. External Data Sharing:

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

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

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

Retention Period	Retention Justification
Surveillance Video is currently stored for 3-4 months. Real Estate Department is in the process of upgrading storage to comply with 1 year of video storage per the Surveillance policy requirement. Video approved for export (based on incidents and case number) is provided to the approved party, who are	Video storage capacity is currently 3-4 months, based on available storage capacity. Additional storage is in the process of being purchased to allow for 1 year of storage as mandated per the surveillance ordinance requirements.

responsible for storing the video of the incident.	

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Exceptions to Retention Period - PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Video approved for export (based on incidents and case number) is provided to the approved party. The approved party are responsible for storing the video of the incident and for the duration of that storage.

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

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

- Practices: Video footage is overwritten at the end of the defined storage length. Animal Care and Control footage is currently stored for between 3 and 4 months (exact storage length is affected by amount of motion, captured on record on motion cameras.) Once storage capacity is increased to 1 year, stored video footage will be overwritten after 1 year.
- Processes and Applications: Under approved uses of the Animal Care and Control Surveillance policy, some visual identifying data is necessarily retained in order to identify those involved in incidents captured by cameras.

Department Compliance

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

The department provides limited access to all employees via real-time security monitors. Only select employees can access recordings for the authorized uses as described: Director, Deputy Director, Operations Manager, Principal Administrative Analyst, and Animal Control Captain and Lieutenants. Access is gained through password protected user accounts. The accounts are established by Media Services.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

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

The Real Estate Department is the custodian of Record for all data and has an approved Surveillance Technology Policy which governs the export and release of video.

Oversight Personnel

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

- Director – 0962
- Deputy Director – 0952
- Operations Manager – 0923
- Principal Administrative Analyst – 1824
- Field Services Captain – 3379
- Field Services Assistant Supervisors - 3378

Sanctions for Violations

Sanctions for violations of this Policy include the following:

Violations of the STP will follow established employee disciplinary procedures. The 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

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 Inquiries

The public may register complaints or concerns by emailing the department at ACC@sfgov.org, which will be brought to the immediate attention of the Director.

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

The general inbox for SFACC is monitored and triaged daily.

Inquiries from City and County of San Francisco Employees

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.