Surveillance Technology Policy

Human Services Agency
Security Cameras

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 Security Camera System itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Surveillance Technology Policy ("Policy") defines the manner in which the Security Camera System (fixed or mobile) will be used to support the Human Services Agency (HSA) operations.

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

POLICY STATEMENT

The Human Services Agency (HSA) will limit their use of Security Camera to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Administrative investigations of employee misconduct.
2. Theft/destruction of HSA property including vehicles, documents, building premises, etc…
3. Investigation of assaults against staff and members of the public, all welfare-related crimes, general crimes occurring at HSA sites.

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.

All data collected by surveillance cameras is the exclusive property of the City and County of San Francisco. Under no circumstance shall collected data be sold to another entity.

BUSINESS JUSTIFICATION

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

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
X	Criminal Justice	Safeguards and protects public property. Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
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	The camera system's live feeds are monitored by on site contract security officers, enabling them to identify potential threats to staff and public in real time. The cameras augment the security officers' ability to respond quickly and efficiently with fewer officers required to manage specific building floor areas.
X	Time Savings	The system's storage capacity similarly increases the effectiveness of the agency's small investigations team in responding to complaints made against staff, members of the public and security personal, investigate crimes that are reported after they have occurred.
X	Staff Safety	Security cameras help identify violations of City Employee's Code of Conduct, 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	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Service Levels	Security cameras will enhance effectiveness of incident response and result in 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.

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	WMV	Level 3
Date and Time	MP4 or other format	Level 3
Geolocation data	TXT, CSV, DOCX	Level 3

Notification: Departments shall not notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas.

Access: Access to stored surveillance video is limited to HSA law enforcement unit for use in official logged investigations only.

Access to recordings and live views is limited using username/password access control, and requires access to a workstation computer on the agency's network.

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.

- 2966 – Welfare Fraud Investigator

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

- Microbiz Security Co. for system maintenance and installation of camera and recording equipment

B. Members of the public

HSA 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) 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.

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

- Network video recorder systems are username/password protected and are secured in locked closets in non-public areas inside HSA buildings. All transmission, both from cameras to recorders and from recorders to investigator' and guards' workstations occur over the agency's secure internal network and dedicated data circuits.
- Hard drives are password protected and are secured in locked closets in non-public areas inside HSA buildings. Stored and live images are transmitted via the Department's secure internal digital network to

investigators' work computers. These devices are likewise password protected and located in investigations division offices.

-

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 Security Camera Systems will act in conformity with this Surveillance Technology Policy.

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

Each department that believes another agency or department receives or may receive data collected from its use of Security Cameras should consult with its assigned Deputy City Attorney regarding their response.

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

X	Confirm the purpose of the data sharing aligns with the department's mission.
X	Consider alternative methods other than sharing data that can accomplish the same purpose.
X	Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
X	Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
X	Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
X	Ensure 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 Security Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Security Camera images may be live-streamed or shared by alternative methods to the following agencies:

- Within the operating Department
- Police
- City Attorney
- District Attorney
- Sheriff
- On request following an incident.

Data sharing occurs at the following frequency:

- As needed but typically 0-1 time a year. Only video images shared, no audio.

B. External Data Sharing:

- No data is shared with outside entities

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:

- Security Camera data will be stored for one (1) year to be available to authorized staff for operational necessity and ready reference.

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

- Justification: This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

Data 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

☐ Software as a Service Product

☐ Cloud Storage Provider

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

- Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.
- HSA may also use Adobe Premier "Scrubbing" software to remove welfare recipient images that are recognizable but not material to a particular investigation.

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

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. Complaints of misuse are investigated and referred to the Department's Human Resources Division as appropriate for follow-up.

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

- HSA Privacy Officer

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.

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:

General compliant and comment forms are available in public areas of all HSA buildings. All complaints are processed on a flow 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.