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. Live monitoring.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

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.

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

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras 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 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:	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 • Human Services Agency, Information Technology *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.
- 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 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.
	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."

1. A description of the product, including vendor and general location of technology.

The following is product inventory and manufacturer's description:

- 1235 Mission:
  - HONEYWELL MAXPRO – RECORDER
  - PELCO DX8100 – RECORDER
  - ANALOG CAMERAS (25)
  - IP CAMERAS (16) – HONEYWELL IP AND 2 AXIS P3708-PVE
- 1440 Harrison:
  - SALIENT – RECORDER
  - IP CAMERAS (12) – HONEYWELL IP
- 170 Otis:
  - HONEYWELL – RECORDER
  - ANALOG CAMERAS (31) – SONY
  - NAS (VM) – RECORDER
  - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
  - DIGITAL IP CAMERAS (6) – VIVOTEK
- 2 Gough:
  - NAS (VM) – RECORDER
  - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
  - DIGITAL IP CAMERAS (2) - VIVOTEK
- 3120 Mission:
  - HONEYWELL – RECORDER
  - ANALOG CAMERAS (4)

- Manufacturers' Product Descriptions:
  - VIVOTEK - VIVOTEK Inc. was founded in February 2000. The Company markets VIVOTEK solutions worldwide, and has become a leading brand in global security surveillance. To fulfill its global strategic footprint, VIVOTEK is committed to building an ecosystem for the IP surveillance industry, and looks forward to long term collaboration and growth with all partners in our shared pursuit of a safe and secure society.
  - PELCO DX8100 - The DX8100 Series digital video recorders (DVRs) are professional security-level DVRs based on a new and innovative hardware platform that is powered by unparalleled and unique high-performance

software. As the security requirements of your business expand into multiple sites and become more diversified, you need a professional DVR that you can quickly and effortlessly increase the channel and recording capacity. •The DX8100 is interoperable with your existing DX8000 DVRs, allowing you to build upon your existing security system. A DX8100 client can operate and administer both the DX8100 and DX8000 within the same network.•When you need to quickly and easily add more security cameras, the new DX8100-EXP 16-channel expansion unit extends the 8- or 16-channel DX8100 to 24 or 32 channels. With or without the channel expansion unit, all of the cameras can now take advantage of the increased frame rate of 2CIF and 4CIF recording. The DX8100 records video up to 480 images per second ips at a maximum CIF image size. •If your security project requirements increase storage capacity, you can extend internal storage up to 3 TB. With the optional DX9200 HDDI, you can further increase the DX8100 storage capacity. Alternately, you can use the DX9200 HDDI as a redundant RAID solution. •As your audio security needs grow, use the DX8108-AUD or DX8116-AUD audio option to add a total of 8 or 16 audio inputs. •Sophisticated video security applications require a network of DVRs to monitor multiple locations. The 10/100/1000 megabit Ethernet port supports today's high-speed networks. You can network your DX8100 and DX8000 systems and remotely operate the DVRs for continuous, motion detection, alarm, ATM/POS, normal scheduled recording, and administer and view live and playback video. For time-critical security applications, you must ensure that all video recordings are synchronized to an accurate time source. The DX8100 supports the network time protocol (NTP), which allows you to synchronize all networked DX8100s to one NTP time server.

- HONEYWELL MAXPRO VMS is an enterprise-class video management and hybrid solution. It enables you to operate the traditional analog, network and IP based video equipment in the same surveillance network. You can deploy thousands of cameras in number of locations, and add many video devices such as recorders and monitors.
- NAS VIRTUAL MACHINE (VM) – The VM is powered by Intel® Xeon® dual core CPU E5-2670 0 @ 2.60GHz x-64 processor, 64-bit Operating System, 4.00 GB of RAM, 75 GB of hard drive space.

- SALIENT NVR SERVER – Salient's hybrid NVRs are industry-leading, value-oriented digital video surveillance systems. Power-built for the rigors of continuous duty operation using advanced components, the 1U rack-mountable PowerPro hybrid NVR delivers the reliability and processing power required for mission critical video surveillance. PowerPro offers a Single Intel Xeon processor with 16GB of memory and up to 48TB of video storage delivering high reliability and processing power. Providing up to 32 analog direct connect channels, this hybrid NVR supports IP and analog cameras in a 1U rack mount unit.
- VIVOTEK's FD8169A is an easy-to-use fixed dome network camera specifically designed for indoor security applications, with a 2MP sensor enabling a viewing resolution of 1920x1080 at a smooth 30 fps. Dynamic and highly adaptable. The FD8169A is an all-in-one camera capable of capturing high quality video at high resolutions of up to 2 Megapixels. It also features POE, Real-time H.264, MJPEG Compression (Dual Codec), Removable IR-cut Filter for Day & Night Function, Built-in IR Illuminators effective up to 20 Meters, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Smart IR Technology to Avoid Overexposure, Supports ONVIF Standard to Simplify Integration and Enhance Interoperability, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- VIVOTEK's FD8182-F2 is an economic professional indoor fixed dome network cameras in VIVTOTEK's 5MP V-Pro Lite series. Design to provide higher resolution and sharper image with more detail, the FD8182-F2 offers up to 15 fps at 5-Megapixel or 30 fps at 1080p resolution. With powerful 3D Noise Reduction technology and Smart Stream technology, the FD8182-F2 can also optimize resolution for a desired object or area to maximize efficiency of bandwidth usage. Other features include POE, Built-in IR Illuminator Effective up to 30 Meters, WDR Enhancement for Unparalleled Visibility in Bright and Dark Environments, Smart Stream to Optimize Bandwidth Efficiency, 3D Noise Reduction for Low-light Conditions, Two-way Audio, PIR motion sensors, Video Rotation for Corridor View, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security

- VIVOTEK's IB8360-W (wireless) is a stylish 2-megapixel mini outdoor bullet network camera, specifically designed for boutique retail applications. Delivering a resolution of 1920x1080 at 30 fps, having IR illuminators effective up to 12 meters, and including SNV technology for low light environments, the remarkable cameras provide users with superior image quality around the clock. It also provide built-in IR Illuminators up to 12 meters, Smart IR Technology to Avoid Overexposure, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Weather-proof IP66-rated Housing, Built-in 802.11 b/g/n WLAN, Compact Size, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- HANWHA PNM SERIES MULTI-SENSOR 360 – Network vandal outdoor Multi-sensor Multi-Directional dome camera, (5MP X 4 sensors) 20MP @ 30fps WDR off/on, motorized vari-focal Lens 2.6x (3.6 ~ 9.4mm) (102.5˚ ~ 38.7˚), triple Codec H.265/H.264/MJPEG with WiseStream II technology, 120dB WDR, Defocus detection, built in analytics, true D/N, 4x SD card, hallway view, HLC, Defog detection, DIS(Gyro sensor), 12VAC/HPoE (power adaptor is included), IP66/IK10, -40°C ~ +55°C (-40°F ~ +131°F)
- HANWHA X SERIES DOME – WiseNet X powered by WiseNet 5 network IR indoor dome camera, 5MP @30fps WDR off/on, 3.7mm fixed focal lens (97.5°), H.265/H.264/MJPEG, WiseStream II compression technology, 120dB WDR, USB port for easy installation, advanced video analytics and sound classification, High powered IR LEDs range of 98', True D/N, dual SD card, hallway view, HLC, defog detection with simple focus, DIS , 12VDC/24VAC/PoE, IK08 rated
- AXIS P3708-PVE - is a fixed dome network camera with three sensors. It gives you a 180º panoramic overview of large areas using a single camera. And it's perfect for use in challenging light conditions, both during the day and at night.
- HONEYWELL – HD4DIRH - 700TVL VFAI WDR TDN IR Mini Dome – Honeywell 960H System Series of cameras provides a wide range of high-quality, feature rich video surveillance options for indoor, outdoor, and low-light applications. 1/3" 960H CCD image sensor, ultra-high resolution image (700TVL), 3D digital noise reduction, digital wide dynamic range, backlight compensation and highlight masking, smart IR technology for even distribution of the IR, 2.8-12 mm varifocal auto iris (VFAI) lens, true day/night

function for vivid color pictures by day and clear black and white pictures at night, excellent low-light performance (0.19 lux color, 0 lux with IR LEDs on), 18 IR LEDs provide up to 50 ft of illumination, depending on scene reflectance, weatherproof, impact-resistant housing (IP66), built-in heater for cold weather operation down to -40 F, breather vent prevents condensation buildup.

- HONEYWELL – HD4D2 – 650 TVL DOME CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE.
- HONEYWELL – H4L2GR1V – 2 MEGAPIXEL DOME IP CAMERA - Full HD 1080p 50/60 fps image with a ½.8"2 MP sensor, WDR up to 120 dB ensures glare-free images, true day/night provides colour images by day and clear black-and-white images at night with ICR, excellent low-light performance with 3D noise reduction, saving storage and bandwidth together with H.265 High Profile codec, low light technology is able to capture high quality colour images in low light environments, 2.7-13.5 mm, F1.6, motorized focus/zoom lens, H.265 plus, H265, H.264 and MJPEG codec, triple stream support, IR LEDs provide up to 50m (150') of illumination in dimly lit or night time scenes (depending on scene reflectance), smart IR technology provides even distribution of IR, waterproof (IP67) and IK10 vandal resistant camera housing, -40C to 60C working temperature, ONVIF Profile S, G & Q compliant, security features include individual signed certificates and data encryption, cameras can be retrofitted on many existing DVR/NVR installations without requiring additional storage, built-in PoE eliminates separate power supply and associated wiring; 24 V AC/12 V DC inputs where PoE is unavailable, 12 VDC/2W output, supports up to 128 GB micro SDHC (Class 10) card for local video storage when network is interrupted.
- ARECONT – AV2256PM – 2 MEGAPIXLE DOME IP CAMERA - The AV2256PM MegaDome® 2 series network camera is part of Arecont Vision's Wide Dynamic Range line of H.264 MegaDome® 2 series cameras. This fully compliant implementation of H.264 (MPEG 4, Part 10) provides full 1920 x 1080 megapixel resolution at full video frame rates of 32fps. The AV2255AM camera line provides an all-in-one solution with integrated 1080p resolution camera, remote focus, remote zoom, motorized P-iris lens, and IP66 and vandal resistant dome enclosure. With the features of Casino mode, ONVIF Profile S, PSIA conformance, privacy masking, extended motion detection and

flexible cropping, the AV2256PM is a high sensitivity, PoE (IEEE 802.3af) compliant camera. Built with Arecont Vision's massively-parallel MegaVideo® technology, this camera offers over six times the resolution of standard resolution IP cameras with the ability to output full real-time frame rates and deliver the high quality megapixel imaging for both indoor and outdoor applications.

- AXIS – P3707-PE – 8 MEGAPIXEL MULTI-SENSOR 360-DEGREE IP CAMERA - AXIS P3707-PE comprises four camera heads that can be repositioned along a circular track to point in the desired viewing direction. Each camera head can be individually tilted and adjusted to provide a 108° to 54° horizontal field of view for either wide or zoomed-in views. The camera heads can be rotated to support Axis' Corridor Format for optimal coverage of vertically oriented scenes. A specially designed clear cover, with no sharp edges, allows for undistorted views in all directions. AXIS P3707-PE supports individually configurable video streams for each camera head, as well as quad-view streaming, enabling 1080p resolution videos at 12.5/15 frames per second and 720p videos at full frame rate.
- SONY – EX543 – ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE
- TRIVIEW – TFD-CVSH312A1241IR – DOME ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
   - 2966 WELFARE FRAUD INVESTIGATOR
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.

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.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

See question #1 for specific storage details. When an incident occurs, images may be recovered from the recorder and preserved on DVD diskettes pursuant to the requirements of a given investigation and evidence retention guidelines. Data is stored with case documents in locked file cabinet and/or evidence vault in secure agency office facility.

5. Is a subpoena required before sharing with law enforcement?
    - Yes