Attachment 2

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 ballot processing and election-related operations.
~~2. Live monitoring of Department staff during elections operations.~~
3. Live streaming ~~footage~~ of ballot processing and election-related operations.
~~3. Recording of video and images of Department staff during elections operations.~~
4. Reviewing camera footage in the event of an incident.
~~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~~ the Department to provide remote ~~election~~ observation of election activities while minimizing deployment of personnel to staff each observation area to support potential observers.
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	Web streaming cameras may run 24/7~~/365~~ during an election cycle regarding ballot processing and election-related operations. Cameras linked to the security system in the Department's Warehouse operate when the system is engaged. Data resolution can be set by level and is currently set to standard resolutions. ~~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. Any ~~Recorded~~ footage that is recorded is accessed only in response to an incident and is automatically deleted ~~10~~ up to 4 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 from security system at the Department's Warehouse may 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.
- ~~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.
   - Indoor security cameras. Deployed during ~~E~~election cycle at Department of Elections for live streaming ballot processing and election--related operations in City Hall and the Department's Warehouse, and to record incidents occurring after-hours in the Warehouse
   - ~~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 IT Operations Support Admin II
     - 1043 IS Engineer-Senior
     - 0962 Dept Head II
     - 0952 Deputy Director II
     - 0951 Deputy Director I
     - ~~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, -415-558-6100~~415-554-4375~~,
     SFVote@sfgov.org, Contact form: https://sfelections.gov~~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.~~Recordings are automatically saved to a cloud based platform for a period of up to 4 days as part of a subscription plan. After the retention period, the recordings are automatically deleted.

5. ~~Questions & Concerns~~