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 department 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

City departments using this policy 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.
BUSINESS JUSTIFICATION

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

- Education
- Community Development
- Health
- Environment
- Criminal Justice
- Jobs
- Housing
- Other

- Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
- Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
- Better management of city assets by leveraging remote condition assessment. Improvement of overall situational awareness.

In addition, the following benefits are obtained:

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Savings</td>
<td>Department Security Camera Systems will save on building or patrol officers.</td>
</tr>
<tr>
<td>Time Savings</td>
<td>Department Security Camera Systems will run 24/7, thus decreasing or eliminating building or patrol officer supervision</td>
</tr>
<tr>
<td>Staff Safety</td>
<td>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.</td>
</tr>
<tr>
<td>Data Quality</td>
<td>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.</td>
</tr>
<tr>
<td>Service Levels</td>
<td>Security cameras will enhance effectiveness of incident response and result in improved level of service.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Data Type(s)</th>
<th>Format(s)</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video and Images</td>
<td>MP4, AVI, MPEG</td>
<td>Level 3</td>
</tr>
<tr>
<td>Date and Time</td>
<td>MP4 or other format</td>
<td>Level 3</td>
</tr>
<tr>
<td>Geolocation data</td>
<td>TXT, CSV, DOCX</td>
<td>Level 3</td>
</tr>
</tbody>
</table>

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:

- Information on the surveillance technology
- Description of the authorized use
- Type of data collected
- Will persons be individually identified
- Data retention
- Department identification
- 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 and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident.

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 cybersecurity 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 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.

The 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.

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:

- Security Camera data will be stored for a minimum of 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:

- 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:

- 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.”
Report Summary Information

Name VB Security Camera
Respondent Karen Burke-Hill
Date Completed

Report Question Responses

1 Change in Authorized Use Cases

1.1 In the last year, did your department have use cases which differed from your “approved use cases” in your BOS-approved policy?
Response No

2 Change in Authorized Job Titles

2.1 Does the list of “authorized job titles” in your BOS-approved policy need to change? (i.e. Do you need additional job titles to be authorized to access the data, or do you need to remove any current job titles?)
Response Yes

2.2 Please provide an updated list of authorized job titles.
Response
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

Comments
Karen Burke-Hill
Adding the Managing Director and Assistant Managing Director to the list of authorized job titles.

2.3 Why have the job titles changed?
Response
The job titles of Managing Director and Assistant Managing Director have been added. These titles were omitted from the original policy in error.

3 Change in Number and/or Type of Technology

3.1 Sections 4-6 cover changes in the number or type of technology addressed by the Surveillance Technology Policy.
Please review and respond according to your department's current situation.

4 Replacement of Old Technology
4.1 Has any technology listed in the policy been replaced?

Response

Yes

Comments

Karen Burke-Hill

Upgraded Avigilon Control Center Server software from version 6.8.6.4 to version 7. Camera sensors (lenses) are being replaced with narrower angle models to improve image quality. A Mobotix S15 model camera controller failed and needed to be replaced. The original model controller is no longer available and so the replacement is a model S16. No changes to the system alter the functionality or use of the Veterans Building Security Camera System. The purchases for software and hardware were submitted for Surveillance Technology review and all were deemed exempt.

5 Addition of New Technology

5.2 Why has the technology been added?

Response

Security Camera Server software needed to be upgraded to latest version. Mobotix 103-degree and 90-degree sensor modules (lenses) have been purchased to replace Mobotix wide-angle sensor modules which provide distorted views. A Mobotix S15 Flex Mount camera module failed and was replaced with an S16 model. The original model is no longer available.

5.3 Please list technology which was added (include manufacturer and model information).

Response

Avigilon ACC 7 Server Software upgrade
MOBOTIX - Sensor module (lens) S16/M16, S15/M15 with HD premium lens (103 degree 6MP)
MOBOTIX - Sensor module (lens) S16/M16, S15/M15 with HD premium lens B041 (9 degree 6MP)
Mobotix S16 Camera Module (controller)

Note: A Surveillance Technology Ordinance review deemed each of these acquisitions as exempt.

5.4 Please list how many units have been added.

Response

No units have been added. Only an upgrade to the software and replacements for existing equipment have been made.

6 Ceased Operation of Technology

6.1 Is any technology listed in the policy no longer in use?

Response

No

7 Services or Equipment Sources

7.1 List any and all entities, companies or individuals which provide services or equipment to the department which are essential to the functioning or effectiveness of the Surveillance Technology (list “N/A” if not applicable):

Response

N/A

8 Surveillance Technology Goals
8.1 Has the surveillance technology been effective at achieving its identified purpose?

Response

Yes

8.2 In 3-5 sentences, please explain how the technology has or has not been effective

Provide quantitative data to support your response. This should include crime statistics for the radius where the technology operates if that was a motivating factor in acquiring the surveillance technology.

Response

The Veterans Building Security Camera System has been effective in enhancing Security staff’s ability to monitor and respond to incidents in the Veterans Building. Monitoring of live views increases situational awareness. This allows Security Officers at the Security Camera Workstation or Supervisors to radio roving staff to investigate suspicious or problematic activities detected on the premises.

Access to recorded footage has been useful in the investigation of incidents by the Director of Security.

A system log listing access to recorded Security Camera data for the period of 10/1/21 through 9/30/22 is attached. This log indicates times and dates when recorded footage was accessed for investigation purposes following an incident. (Crime statistics for the radius where the technology operates was not a motivating factor in acquiring this surveillance technology.)

Data Sharing

9.1 Has data acquired through the surveillance technology been shared with entities outside of the department?

Response

No

9.4 Was the data shared with entities outside of city and county government?

Response

No

Accidental Receipt of Face Recognition Data

10.1 Did your department inadvertently or unintentionally receive, retain, access or use any information obtained from Face Recognition Technology?

Response

No

Complaints

11.1 Has your department received any complaints and/or concerns from community members about this surveillance technology?

Response

No

Violations

12.1 Were there any violations of the Surveillance Technology Policy or Surveillance Impact Report, reported through community members, non-privileged internal audits, or through other means in the last year?

Response

No
12.4 Has your department conducted any internal audits of the technology?
Response
No

13 Statistics and Information about Public Records Act Requests
13.1 Has your department received any public records act requests for this surveillance technology?
Response
No

14 Total Annual Costs for the Surveillance Technology
14.1 List the number of FTE (new & existing).
Response
.025 of a 1093 IT Operations Support Administrator III-IT Manager's time

14.2 Are there one-time costs for Fiscal Year 2022-23?
Response
No

14.15 Are there annual costs for Fiscal Year 2022-2023:
Response
No

14.28 What source of funding will fund the Surveillance Technology for FY 2022-2023?
Response
War Memorial Operating Budget

14.29 Have there been any changes to the one-time costs from your department's approved Surveillance Impact Report?
Response
No

14.31 Have there been any changes to the annual costs from your department’s approved Surveillance Impact Report?
Response
No

14.32 Why have the annual costs changed?
Response
N/A

15 Annual Inventory Check
15.1 **Note:**

In 2019, all departments were asked to compile a list of surveillance technologies which their department uses. Since then, departments have been asked to contact COIT about new technologies for a surveillance technology review via the Surveillance Technology Ordinance Form in ServiceNow. Please feel free to reference the current Surveillance Technology Inventory for your department to help you answer the following questions.

15.2 **Is the Surveillance Technology Inventory for your department current and accurate?**

**Response**

No

**Comments**

Karen Burke-Hill

Software has been upgraded and one camera module (controller) has been replaced with a new model and two more camera modules of the new type are pending.

Updated inventory is below:
- Cameras: Mobotix S15D and S16 FlexMount Dual Cameras
- Server: Rasilient ApplianceStor90
- Software: Avigilon Control Center Server Std Smart Plan (Current version: ACC7)

10/26/2022 03:08 PM

15.3 **Are there any technologies which need to be removed from the inventory because the department no longer uses the technology?**

**Response**

No

15.5 **Are there any technologies which need to be added to the inventory because they are non-exempt surveillance technology?**

**Response**

No

**Comments**

Karen Burke-Hill

All changes to the system - upgraded software and new model sensor modules (lenses) - were deemed exempt under Surveillance Technology Ordinance review.

10/26/2022 03:19 PM

15.7 **Are there any other inaccuracies with your department’s inventory which has not already been addressed?**

**Response**

No

15.9 **You have completed the Annual Surveillance Report:**

*Congratulations and see you next year!*