Surveillance Technology Policy

Johnson Controls P2000 Security Management System - Video System
San Francisco Public Library

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 San Francisco Public Library (SFPL) system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Johnson Controls P2000 Security Management System - Video System will be used to support department operations.

This Policy applies to all Department personnel that use, plan to use, or plan to secure the Johnson Controls P2000 Security Management System - Video System, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with SFPL are required to comply with this Policy.

POLICY STATEMENT

The use of Johnson Controls P2000 Security Management System - Video System technology for the San Francisco Public Library is limited to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring to protect safety of SFPL staff, patrons and facilities.
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 SFPL operations, the Johnson Controls P2000 Security Management System - Video System promises to help with:

☐	Education	
☐	Community Development	
X	Health	Protect safety of SFPL staff, patrons and facilities while promoting an open and welcoming environment.
☐	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or other authorized persons following an incident or upon request.
☐	Jobs	
☐	Housing	
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	Security cameras will save on need for building or patrol officers.
X	Time Savings	Security cameras will run 24/7/365, thus decreasing need for building or patrol officer supervision.
X	Staff Safety	Security cameras help identify violations of City Employee's Code of Conduct, SFPL Patron Code of Conduct, 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 the Johnson Controls P2000 Security Management System - Video System 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 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 cyber security requirements. - Audits: A data access log will be maintained by the Department for all the Johnson Controls P2000 Security Management System - Video System 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 the Johnson Controls P2000 Security Management System - Video System 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 Johnson Controls P2000 Security

Management System - Video System should consult with its assigned Deputy City Attorney regarding their response.

Before sharing data with any recipients, SFPL 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.

SFPL 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 Johnson Controls P2000 Security Management System - Video System footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Johnson Controls P2000 Security Management System - Video System images may be live-streamed or shared by alternative methods to the following agencies:

- Within the San Francisco Public Library
- 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, via formal process, order or subpoena, per the San Francisco Public Library Privacy Policy.

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:

- Johnson Controls P2000 Security Management System - Video System data currently will be stored for a minimum of four (4) months as SFPL seeks to expand server capacity to meet State requirements of a minimum of one (1) year 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.

The Johnson Controls P2000 security management system (https://author.johnsoncontrols.com/en_gb/buildings/security-and-fire-safety/access-controls) helps organizations achieve maximum security while increasing efficiencies and lowering costs. Built on open standards and compatible with virtually any third party program, the P2000 can integrate multiple businesses, buildings and security systems to achieve interactive, real-time security management. The P2000's built-in web browser allows users to access the platform from a central location — or remotely, through web-connected devices.

Security cameras record and retain video footage of public and non-public spaces within and on the exterior of 15 facilities of the San Francisco Public Library. That video footage is stored on a server system that lives on the 6th Floor of the Main Library. Video footage is then accessible for review by authorized users within the organization, local law enforcement, including the Sheriff's Department (per existing MOU), or, can be shared externally, upon request, given policy constraints enumerated herein.

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

Access to SFPL security camera data is restricted to staff with specific needs related to protecting the safety of SFPL staff, patrons and facilities while in or around library locations. Training and user access restrictions will prevent unauthorized access and use of the security camera software, including misuse.

Access to the information includes 23 8207 Grounds and Patrol Officers, 3 8211 Ground and Patrol Supervisors, the 0923 Manager of Security Operations and Emergency Planning, the 0923 Manager of Buildings and Engineering, the 0932 Director of Facilities, the 0953 Chief Operating Officer and the 0964 City Librarian. The Sheriff's Department also has access to security camera footage, per existing MOU for onsite support at the Main Library.

All other staff requesting access to this data must make a formal written request to the Facilities Division, pending approval by the Chief Operating Officer or the City Librarian. These protocols ensure limited access to security camera footage among SFPL staff.

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: Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library, 100 Larkin Street, San Francisco 94102. They can also contact the library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

City and County of San Francisco Employees: All questions regarding this policy should be directed to the employee's supervisor or to the division chief. 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 division chief.

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

Security camera data is stored on a local server at the Main Library and is maintained remotely by Johnson Controls, Inc. The retention period for this data is related to server capacity, and it is currently holding approximately 4 months of footage before being overwritten. SFPL recognizes that there is a 1-year storage requirement per the California Public Records Act, and is working toward increasing capacity to comply with state law.

5. Questions & Concerns

Public: Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library. They can also contact the library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

City and County of San Francisco Employees: All questions regarding this policy should be directed to the employee's supervisor or to the division chief. 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 division chief.