Surveillance Technology Policy

Camera Management and Video Monitoring System
Fine Arts Museum

The City and County of San Francisco (CCSF) value 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 Camera Management and Video Monitoring 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 Department's mission is to connect our visitors with local and global art in order to promote their knowledge of and curiosity about the past, deepen their engagement with the art and ideas of today, and stimulate their creative agency in their own futures.

The Surveillance Technology Policy ("Policy") defines how the Camera Management and Video Monitoring System will be used to support this mission by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all department personnel that use, plan to use, or plan to secure Camera Management and Video Monitoring System, including employees, contractors, and volunteers. In addition, employees, consultants, volunteers, and vendors must comply with this Policy while working on behalf of the City or with the Department.

POLICY STATEMENT

The authorized use of Camera Management and Video Monitoring System technology for the Department is limited to the following use cases. In addition, it is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Live video monitoring feeds.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage or images to external 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 technology 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 biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on the preceding sentence's categories.

BUSINESS JUSTIFICATION

Surveillance Oversight Review Dates
PSAB Review: December 9, 2022; Recommended with changes.
COIT Review: TBD
Board of Supervisors Review: TBD

Camera Management and Video Monitoring System supports the Department's mission and provides essential operational value in the following ways:

The surveillance technology protects the City's valuable assets (art and building) and supports the Security Staff in doing their job well, increasing productivity and safety. In addition, it reduces overall liability and risk for the City and assures our ability to give the public access to the unique art collection and world-class exhibitions.

In addition, the Camera Management and Video Monitoring System benefit residents in the following ways:

	Benefit	Description
☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
☐	Criminal Justice	
☐	Jobs	
☐	Housing	
X	Public Safety	Assures our ability to give the public access to the unique art collection and world-class exhibitions
☐	Other	

Camera Management and Video Monitoring System will benefit the department in the following ways:

	Benefit	Description
☐	Financial Savings	
☐	Time Savings	
X	Staff Safety	It allows the museums to review footage related to the damage to the collections.
☐	Data Quality	
☐	Other	

To achieve its intended purpose, Camera Management and Video Monitoring System (from now on referred to as "surveillance technology") provides live views and records motion video footage to network video recorders (NVR). An NVR is a specialized computer system that includes a software program that records video in a digital format to a disk drive. The system is comprised of multiple cameras. The footage is recorded on the NVRs and stored. Data collected or processed by the Fine Arts Museums' surveillance camera system will not

be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability. Department use of surveillance technology and information collected, retained, processed, or shared by surveillance technology must be consistent with this Policy; comply with all City, State, and Federal laws and regulations; and protect all state and federal Constitutional guarantees.

Specifications: The software and firmware used to operate the surveillance technology must be up to date and maintained.

Safety: Surveillance technology must be operated safely. Surveillance technology should not be used to infringe on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect the 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.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Video/audio	Exe, Avi	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 per Section 19.5 of the Administrative Code. Department notifications shall identify the type of technology 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
- Department identification
- Contact information

Access: Before accessing or using data, authorized individuals receive training in system access, operation, and instruction regarding permitted and prohibited uses.

Before public use, data must always be scrubbed of PII.

Access to live views and recorded footage is restricted to specifically trained personnel.

The following roles and job titles are authorized to view live video monitoring feeds:

- 8202 - Security Guard
- 8226 - Museum Guard
- 8228 - Museum Security Supervisor
- 8229 - Manager of Security
- 0922 - Associate Director of Museum Security
- 0923 - Director of Museum Security Supervisor

Recorded footage is accessed only in response to an incident. The following roles and job titles are authorized to view recorded video footage:

- 8228 - Museum Security Supervisor
- 8229 - Manager of Security

Members of the public, including criminal defendants, may also request access by submitting a request according to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

The Fine Arts Museum will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the federal and State Constitutions requirements, and federal and state civil procedure laws and rules.

Collected data 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 restrictions. Any damages resulting from the use of public data are disclaimed, including by criminal defendants.

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.

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

- Encryption: Data retained by the Department will be encrypted. The Department may retain raw data only for the authorized use case of sharing with external law enforcement or the public.
- Storage: Any third-party service provider use must meet City's cybersecurity requirements.
- Audits: The Department will maintain a data access log for all Security Camera data that is processed and utilized. This log will include but is not limited to the following:
    - Date and time data was initially collected or obtained
    - Reasons or intended use for the data
    - The department or entity requesting the data

- The date and time of access to raw data
- The outcome of data processing

Data Sharing: The Fine Arts Museum will endeavor to ensure that other agencies or departments that may receive data collected by the Fine Arts Museum's Camera Management and Video Monitoring System Camera Policy will act in conformity with this Policy.

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.

The Fine Arts Museum shall ensure proper administrative, technical, and physical safeguards before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security)

The Fine Arts Museum shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a person, data concerning health or data concerning a person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies 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 following the department's data policies.

X Review 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 San Francisco's Sunshine Ordinance.

X Ensure data will be shared cost-efficiently and exported in a clean, machine-readable format.

The Fine Arts Museum Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the federal and State Constitutions requirements, and federal and state civil procedure laws and rules.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Data Type	Data Recipient
In the event of an incident, historical recorded footage	City Attorney Office, Human Resources Department, external Law Enforcement

Data sharing occurs at the following frequency:

- Upon request and only in the event of an incident

B. External Data Sharing

The department only shares data with external law enforcement agencies by way of a court order.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

The Department's data retention period and justification are as follows:

Retention Period	Retention Justification
Data is retained for three months.	Available to authorized staff for operational necessity and ready reference.

PII data shall not be kept in a form that permits the identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- If data is associated with an incident, it may be kept longer than the standard retention period. The nature and severity of the incident determines the retention period. Departments must establish appropriate safeguards for PII data stored for more extended periods.

Data will be stored in the following location:

X 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:

Practices:

- Data is automatically recorded over and elapses after three months

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.

At the very least, the Department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting or regularly requiring data access receive appropriate training before granting access to systems containing PII.

Staff is trained to monitor the cameras, including rotating between cameras, identifying suspicious activity, reporting suspicious activity, and responding to dispatch officers.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The department will continue to follow the protocols and work with Security Management and IT Management to ensure compliance.

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third parties:

- Director of Information and Technology
- Director of Museum Security Services (0923)

Sanctions for violations of this Policy include the following:

Each situation is evaluated in consultation with Human Resources. The appropriate action will be taken proportionate to the severity of the offense.

If Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B. In that case, 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.

EXCEPTIONS

Only in exigent circumstances or circumstances where external law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained, or processed by the surveillance technology be shared with external law enforcement.

DEFINITIONS

Personally Identifiable Information:	Information can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information linked or linkable to a specific individual.
Raw Data:	Information collected by surveillance technology has <u>not</u> been processed and cleaned of all personally identifiable information. In addition, the distribution and use of raw data are tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person requires the immediate use of Surveillance Technology or the information it provides.

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 authorize 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:

Complaints or concerns can be submitted to the Department by:

They can contact the museums directly via email at contact@famsf.org or 415-750-3600.

The Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall assign the complaint to a specific staff member who will look into the complaint

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or 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.