Surveillance Technology Policy

Tenant/Contractor Security Cameras
War Memorial

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 San Francisco Symphony ("Tenant/Contractor") Security Camera System by San Francisco War Memorial & Performing Arts Center ("War Memorial Department", "War Memorial", or "Department") as well as any associated data to which Department is privy, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The San Francisco War Memorial & Performing Arts Center manages, maintains and operates safe, accessible, world-class venues to promote cultural, educational, and entertainment opportunities in a cost-effective manner for enjoyment by the public, while best serving the purposes and beneficiaries of the War Memorial Trust.

The Surveillance Technology Policy ("Policy") defines the manner in which the Tenant/Contractor 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 Tenant/Contractor Security Camera Systems or data, 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

This policy applies to security camera data sharing between War Memorial and the following entities:

- San Francisco Symphony

City departments are limited in their use of security camera equipment and footage that is owned and operated by non-City entities to the following authorized use cases and requirements listed in this Policy only.

Authorized Use(s):

1. Live monitoring internal office space and public area of Davies Symphony Hall.
2. Reviewing camera footage provided by Tenant/Contractor upon request in the event of an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Department's processing of personal data revealing legally protected categories, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership,

gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

BUSINESS JUSTIFICATION

Security Cameras supports the Department's mission and provides important operational value in the following ways:

Cameras: AXIS, MODELS P3327-LV, P3227-LVE, P3807-PVE
Server: EXACQVISION IP04-30T-R2A 30-TB NVR
Software: EXAQ EVIP-01 PROFESSIONAL
Vendor: G4S
Location: SF Symphony surveillance cameras are located in public and office/work areas of Davies Symphony Hall and associated grounds.

Security Cameras will benefit the department in the following ways:

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
X	Criminal Justice	Review video footage after a security incident.
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	Tenant/Contractor Security Camera Systems will save on building or patrol officers. Equipment is owned and operated by non-city entity.
X	Time Savings	Tenant/Contractor Security Camera Systems run 24/7, thus decreasing or eliminating building or patrol officer supervision.
X	Staff Safety	Tenant/Contractor Security cameras help identify violations of 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	Service Levels	Tenant/Contractor Security cameras will enhance effectiveness of incident response and result in an 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.

Data Collection:

Department shall only receive data that is required to execute the authorized use case. All surveillance technology data shared with Department by Tenant/Contractor, 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

Access:

Prior to accessing or using data, authorized individuals within the Department 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.

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.

- 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

The following providers are required to support and maintain the surveillance technology and its associated data to ensure it remains functional:

- GS4, Tenant/Contractor's support vendor

B. Members of the public

Data collected by surveillance technology will not be made generally available to members of the public.

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. 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

Members of the public 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 any PII received from Tenant/Contractor (or shared by Tenant/Contractor) 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 received from Tenant/Contractor from unauthorized access and control, including misuse: - Encryption: Data may be retained by the Department only for the authorized use case of reviewing camera footage in the event of an incident. - Storage: Any use of a third-party service provider by the Department must meet City's cyber security requirements. - Audits: A data access log will be maintained by the Department for all Security Camera data, other than live views, received from Tenant/ Contractor that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons for/intended use of data, department requesting data (if any), date/time of data access, outcome of data processing, as well as date the processed data was delivered to users.

Data Sharing:	Tenant/Contractor is the sole owner and custodian of its Surveillance Technology data. Tenant/Contractor may share such data with the Department or other entities at its sole discretion. The Department will endeavor to ensure that other agencies or departments that may receive data collected under War Memorial's Tenant/Contractor Security Camera Policy will act in conformity with this Surveillance Technology Policy. Data is shared by Tenant/Contractor with the Department on the following schedule: ✓ As needed *A. Internal Data Sharing* Department does not share Tenant/Contractor Security camera data with internal or external recipients. *B. External Data Sharing:* Department does not share Tenant/Contractor Security camera data with internal or external recipients.
Data Retention:	Department may store and retain PII data shared by Tenant/Contractor 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 shared with Department by Tenant/Contractor will be stored only for the period necessary for investigation or litigation following an incident. - Justification: This retention period safeguards PII from inappropriate or unauthorized use by minimizing the period and purposes for which it may be retained. PII data shall not be kept in a form which permits 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): - Security Camera data shared with Department by Tenant/Contractor will be stored only for the period necessary for investigation or litigation following an incident.

	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: Practices: - Data is disposed following the period that it is relevant to an ongoing investigation or litigation. Processes and Applications: - Delete/reformat, wipe, overwrite of existing data, or degaussing.
Contracts and/or Legal Agreements:	The War Memorial Department does not have a contract or legal agreement with a third-party entity governing third-party data use, including but not limited to third party data use, sharing, signage, retention, and/or disposal.
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 on behalf of Department must receive training on data security policies and procedures. - Annual cybersecurity training per COIT policy. - Prior to accessing or using data, authorized individuals within the Department receive instruction regarding authorized and prohibited uses.

COMPLIANCE

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

- On a monthly basis, retained Tenant/Contractor footage or images shall be reviewed to determine its continued relevance for any ongoing investigations or litigation.

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

- 0922, Director of Security
- 8211, Supervisor Building and Grounds Patrol Officer
- 1844, Facilities Administrator

Sanctions for violations of this Policy include the following:

- 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

Third-Party or Tenant/Contractor	Non-City Entity that owns and operates security cameras and shares security camera footage with a City department.
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."

QUESTIONS & CONCERNS

Public:

Complaints or concerns can be submitted to the Department by sending an email to WarMemorialinfo@sfgov.org.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall monitor the War Memorial information email box throughout the day during standard business hours. Any communications to that email address are responded to directly or brought to the attention of responsible staff.

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.