Surveillance Technology Policy

Veterans Building Surveillance Camera System
War Memorial

The City and County of San Francisco values 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 the Veterans Building Surveillance 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 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 way the Veterans Building Surveillance Camera 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 the Veterans Building Surveillance Camera System, 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

The authorized use of Veterans Building Surveillance Camera System technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

Live monitoring.
Review video footage/images in the event of an incident.
Provide video footage/images to law enforcement or other authorized persons following an incident.

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

Security Camera images may be used by War Memorial, law enforcement or the City Attorney to identify an individual in the event of an incident.

BUSINESS JUSTIFICATION

The Veterans Building Surveillance Camera System supports the Department's mission and provides important operational value in the following ways:

The War Memorial Security Division utilizes surveillance technology to increase security officer capacity directly related to public safety. The technology enhances the Department's ability to provide a safe and welcoming environment to patrons, visitors and staff.

In addition, the Veterans Building Surveillance Camera System promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
☑	Criminal Justice	May provide evidence for law enforcement criminal investigations.
☐	Jobs	
☐	Housing	
☑	Other	Public Safety - Assists security officers investigating War Memorial Code of Conduct violations and/or criminal acts. - Provides a mechanism to augment foot patrols, prevent criminal acts and assist anyone requiring emergency help.

Veterans Building Surveillance Camera System will benefit the department in the following ways:

	Benefit	**Description**
☑	Financial Savings	Reduce the number of Security staff needed to secure the Veterans Building.
☐	Time Savings	
☑	Staff Safety	Enhances Security staff's ability to observe patrons, visitors and staff members requiring assistance. May provide an alert and help prevent or mitigate dangerous incidents.
☐	Data Quality	
☐	Other	

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 surveillance technology must be kept up to date and maintained.

<table>
<tr><td>Safety:</td><td>Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.</td></tr>
<tr><td>Data Collection:</td><td>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 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.

Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc.

The surveillance technology collects the following data types and formats:

<table><tr><th>Data Type(s)</th><th>Format(s)</th><th>Classification</th></tr><tr><td>Facial and other physical images</td><td>AVE, AVI, PNG, JPEG, TIFF, PDF</td><td>Level 3</td></tr><tr><td>Timestamp reflecting date and time footage was recorded</td><td>AVE, AVI, PNG, JPEG, TIFF, PDF</td><td>Level 3</td></tr></table></td></tr>
<tr><td>Notification:</td><td>Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

☑ 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</td></tr>
</table>

Access:	All parties requesting access must adhere to the following rules and processes: Prior to use, 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 Security and IT personnel. Recorded footage is accessed only in response to an incident. Department may share data on a one-time, as needed basis following an incident with the following internal recipients: San Francisco Police Department City Attorney's Office *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 The following providers are required to support and maintain the surveillance technology and its associated data to ensure it remains functional: N/A *B. Members of the public* War Memorial 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. 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. 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 any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants. Members of the public, including criminal defendants, 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 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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: Access, including inappropriate access, shall be traceable to individual employees.
Data Sharing:	War Memorial 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. War Memorial will endeavor to ensure that other agencies or departments that may receive data collected by the Security Cameras Policy will act in conformity with this Surveillance Technology 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. War Memorial 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. (See Data Security) War Memorial shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. 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: ☑ Confirm the purpose of the data sharing aligns with the department's mission.

	☑ Consider alternative methods other than sharing data that can accomplish the same purpose. ☐ Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. ☐ Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents. ☐ 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. ☐ Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format. The Department currently participates in the following sharing practices: A. Internal Data Sharing Department shares the data with the following recipients: San Francisco Police Department City Attorney's Office Data sharing occurs at the following frequency: On a one-time, as needed basis following an incident. B. External Data Sharing The Department does not share surveillance technology data with external recipients. Data sharing occurs at the following frequency: N/A To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Share surveillance technology data only with other departments of the City and County of San Francisco, not with external entities. Other City departments are also subject to the City's Surveillance Technology Policy Ordinance and its requirements.
Data Retention:	Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories: • Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely • Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years • Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years

	The Department's data retention period and justification are as follows: 30 days is the standard retention period for Veterans Building Surveillance Camera System data. — This retention period is established in order to provide sufficient time for the discovery and report of an incident by tenants, staff or members of the public. 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): If downloaded and stored separately following an incident for the purpose of ongoing investigations or litigation. Departments must establish appropriate safeguards for PII data stored for longer periods. Data will be stored in the following location: ☑ Local storage ☑ 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 older than 30 days is erased from storage media by automated processes. Processes and Applications: Retention is set to a 30 day limit using settings in Avigilon surveillance camera software.
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, 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 data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

	User training includes instruction in the operation of the system to view live images and to access and search recorded footage. Directions are provided regarding appropriate and inappropriate uses of live images and footage. Training is performed by experienced Security staff or IT staff.

COMPLIANCE

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

The mechanisms to ensure that the Surveillance Technology Policy is followed include internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority and the sanctions for violations of the policy.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

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

Sanctions for violations of this Policy include the following:

- The Department of Human Resources Employee Handbook, as well as the War Memorial Statement of Incompatible Activities, prohibit the use of City resources, including City computers and data, for personal or other non-City purposes. The Veterans Building Surveillance Camera System is considered by the War Memorial to be a City resource. Misuse of surveillance video views or footage may be grounds for disciplinary action.

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.

EXCEPTIONS

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

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.

Raw Data:	Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that 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 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 issues related to privacy should be directed to the employee's supervisor or the Director.

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

The technology's primary functions are to provide live views and record video footage to a dedicated, secure server. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a limited amount of time.

Cameras: Mobotix S15D FlexMount Dual Camera
Server: Rasilient ApplianceStor90
Software: Avigilon Control Center Server v6.8.6.4

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Technology Use:

The War Memorial Security Division utilizes surveillance technology to increase security officer capacity directly related to public safety. The technology enhances the Department's ability to provide a safe and welcoming environment to patrons, visitors and staff.

PII:

Yes

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Live monitoring.

Review video footage/images in the event of an incident.

Provide video footage/images to law enforcement or other authorized persons following an incident.

Rules:
Access to live views and recorded footage is restricted to specific trained Security and IT personnel. Recorded footage is accessed only in response to an incident.

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

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type	Formats STP
Facial and other physical images	AVE, AVI, PNG, JPEG, TIFF, PDF
Timestamp reflecting date and time footage was recorded	AVE, AVI, PNG, JPEG, TIFF, PDF

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title:

- 8207 - Building and Grounds Patrol Officers
- 8211 - Supervisor Building and Grounds Patrol Officer
- 0922 - Director of Security
- 1093 - IT Manager
- 1844 - Facilities Administrator

Department:

War Memorial

If applicable, contractor or vendor name:

N/A

Rules and processes required prior to data access or use:

Prior to use, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

Access to live views and recorded footage is restricted to specific trained Security and IT personnel. Recorded footage is accessed only in response to an incident. System access requires use of a username and password.

7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period

Retention:
30 days

Reason for retention:

This retention period is established in order to provide sufficient time for the discovery and report of an incident by tenants, staff or members of the public.

Deletion process:

Retention is set to a 30 day limit using settings in Avigilon surveillance camera software.

Retention exemption conditions:

Data may be downloaded and stored separately for a longer period for the purpose of ongoing investigations or litigation following an incident.

8. How collected information can be accessed or used by members of the public, including criminal defendants

Will the data be accessible to the public:

No

How it can be accessed:

Data is made available to members of the public only by subpoena.

9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.

Name of agency: San Francisco Police Department and the City Attorney's Office.

Justification:
Data is shared with SFPD when requested for the investigation and/or prosecution of a criminal case. Data shall be disclosed to the City Attorney's Office in response to an official request.

Surveillance technology data is only shared with other departments of the City and County of San Francisco which are, therefore, also subject to the City's Surveillance Technology Policy Ordinance and its requirements.

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Training required:

Yes

Description of training:

User training includes instruction in the operation of the system to view live images and to access and search recorded footage. Directions are provided regarding appropriate and inappropriate uses of live images and footage. Training is performed by experienced Security staff or IT staff.

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to

information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Training required:

Yes

Process for responding to complaints:

The War Memorial Director of Security and Security Supervisors are assigned to oversee Surveillance Technology Policy compliance, and are responsible for responding to complaints.

Oversight process:

- The Department of Human Resources Employee Handbook, as well as the War Memorial Statement of Incompatible Activities, prohibit the use of City resources, including City computers and data, for personal or other non-City purposes. The Veterans Building Surveillance Camera System is considered by the War Memorial to be a City resource. Misuse of surveillance video views or footage may be grounds for disciplinary action.

Compliance personnel titles:

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

Restrictions:
Access to live views and recorded footage is restricted to specific trained Security and IT personnel. Recorded footage is accessed only in response to an incident.

12. 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.

Complaint procedures:

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

Departmental follow-up process:

The War Memorial information email box is monitored 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.