Surveillance Technology Policy

Public Utilities Commission
Unmanned Aircraft Systems (Drones)

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 Unmanned Aerial Vehicles or Drone technology 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: provide our customers with high quality, efficient and reliable water, power, and sewer services in a manner that is inclusive of environmental and community interests, and that sustains the resources entrusted to our care. San Francisco Public Utilities Commission provides retail drinking water & wastewater services to the City of San Francisco, wholesale water to three Bay Area counties, green hydroelectric & solar power to Hetch Hetchy electricity customers, and power to the residents & businesses of San Francisco through the CleanPowerSF program.

The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned Aerial Vehicles or Drone technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Unmanned Aerial Vehicles or Drone technology, 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 Unmanned Aerial Vehicles or Drone technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Construction Management: Examples include inspection of project sites for contract and environmental compliance.
2. Environmental Monitoring & Documentation: Examples include monitoring of vegetation type and health, wildlife, and streams/reservoirs.
3. Inspections: Conducting surveys and assessments of SFPUC properties and assets. Examples include survey of bay and ocean outfalls, inspection of large wastewater collections and power line surveys.
4. Disaster Relief: Drones may be used in disaster relief to record footage of damage and assess the role PUC may play in responding to such disasters.
5. Marketing and Public Education: Drones may be used to capture footage of the watershed, as an example, to be used in public education and/or marketing materials.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: August 4, 2021

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/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

Unmanned Aerial Vehicles or Drone technology supports the Department's mission and provides important operational value in the following ways:

The use of Drone technology enables more efficient use of City resources and improved ability to inspect, manage and protect City infrastructure and natural resources.

In addition, Drone technology promises to benefit residents in the following ways:

X	Education	Education: Drone imagery to promote SFPUC projects and educate the public and on our mission and operations.
☐	Community Development	
☐	Health	
☐	Environment	
☐	Criminal Justice	
☐	Jobs	
☐	Housing	
X	Other	Public Safety: Efficient inspection of critical infrastructure (dams, sewer infrastructure, power lines) helps ensure infrastructure is operating safely, minimizing overall risk of failure.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Drones are more efficient and cost effective than traditional methods. In environmental monitoring example, for an 8,000 ft fountain thistle site, it would take an estimated 120 labor hours to collect data if done by individuals counting plants, using traditional methods, costing an estimated $120,000. With a drone it would take two people less than two days and cost about $22,000, including labor and equipment.

X	Time Savings	Performing manual infrastructure inspections and environmental monitoring adds significant time to operations. See specific fountain thistle example above.
X	Staff Safety	See construction management and inspection examples above. Using a drone to capture imagery keeps staff out of dangerous and compromising situations (high structure inspections)
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, providing improved overall data.

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.
Safety:	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.
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 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 some or all of the following data types:

Data Type(s)	***Format(s)***	***Classification***
Photographic and video data of	JPEG, PNG, MOV, AVI, CSV	Level 2

	assets, landscapes and property
Notification:	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: X Information on the surveillance technology X Description of the authorized use X Type of data collected X Will persons be individually identified X Data retention X Department identification X Contact information
Access:	All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): SFPUC Drone Policy must be reviewed and signed by all SFPUC drone operators and any individuals with access to drone data that may contain Personal Identifiable Information. Contractor Provisions: If entering into a contract with a third party to operate drones, the contract shall include the following requirements: • Ownership and handling of City Data: "City Data" includes without limitation all data collected, used, maintained, processed, stored, or generated by or on behalf of the City, including as the result of the use of the services provided by a contractor. The City retains ownership and rights to City Data, including derivative works made from City Data and the licensing applied to the data. Contractors must treat City Data using the same Privacy and Data Security requirements that apply to CCSF employees. • Unauthorized use prohibited - Engaging in the unauthorized use of drones or activities that are inconsistent with this Policy may be grounds for termination of the relevant contract, as well as applicable monetary fines and penalties. • Signatures – This Drone Policy must be reviewed and signed by all drone operators, including contractors

- Insurance required – Contractor drone operators must provide proof of liability insurance commensurate with current SFPUC insurance requirements for contractors.

The SFPUC shall restrict access to any raw (i.e., unprocessed) drone footage that contains PII to authorized City staff (i.e., authorized employees and contractors) only. Distribution of raw drone data containing PII to other City departments shall be for the purpose of cleansing and processing data only. In all other circumstances, the SFPUC shall not exchange raw drone data containing PII between City departments, or disclose such data to the public, except for exigent public safety needs or as required by law.

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.

- 1770 Photographer, San Francisco Public Utilities Commission: Construction Management Bureau

B. Members of the public

Public Utilities Commission 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.

Data collected by surveillance technology will not be made available to members of the public, including criminal defendants.

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:

- Should PII that is not related to the authorized purpose be incidentally collected through use of drones, the SFPUC shall remove all PII from the raw footage, or destroy the raw footage, within one year of collection. Exceptions to this one-year limit must be supported with documentation and a clear rationale, and maintained by SFPUC staff to be reviewed by COIT.

Data Sharing:	Public Utilities Commission will endeavor to ensure that other agencies or departments that may receive data collected by PUC's Drone technology 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. Public Utilities Commission 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) Public Utilities Commission 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: 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.

- 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 data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

Public Utilities Commission 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 currently participates in the following sharing practices:

A. Internal Data Sharing:

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing:

The department does not share surveillance technology data with other departments or entities outside the City and County of San Francisco.

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:

In accordance with the SFPUC Records Management Policy, data and video footage collected during drone operations will fall into one of the following categories:

1. Permanent Records: Records that are permanent or essential shall be retained and preserved indefinitely. Examples include: Drone video footage data collected for environmental monitoring and documentation.
2. Current Records: Records for which operational necessity, ready reference, convenience or other reasons are retained in the office space and equipment of the SFPUC. Examples include: Drone video footage data collected for construction management and inspections.
3. Storage Records: Records that are retained offsite. Typically, Current or Permanent records that have ceased to have immediate operational value, but which have a retention/lifecycle period that requires continued custodianship. Examples include: Drone video footage data collected for encroachments on the pipeline rights of way; until encroachment is removed.

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): Environmental Monitoring: All data is kept for the lifetime of the project as it informs future trends and management, and is invaluable for monitoring population trends and habitat conditions for rare species. Departments must establish appropriate safeguards for PII data stored for longer 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: Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
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. Drone data collection, dissemination and distribution is explained in SFPUC Drone Policy. All authorized users (staff and contractors) must sign off on policy prior to use.

COMPLIANCE

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

- For Drones, all flights are routed to SFPUC Emergency Planning and Security for approval, then inputted into the Open Data Portal 24 hours prior to flight.
- Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.
    - SFPUC Emergency Planning staff.

Sanctions for violations of this Policy include the following:

- Per SFPUC Drone Policy: "Engaging in the unauthorized use of drones or activities that are inconsistent with this Policy may be grounds for termination of the relevant contract, as well as applicable monetary fines and penalties."

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
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, concerns, or questions may be submitted via the San Francisco Public Utilities Commission website https://www.sfwater.org/

Members of the public can send us an email to info@sfwater.org or call the General Inquiries phone number (415) 554-3289.

They may also send a letter via post to 525 Golden Gate Avenue, 10th floor, San Francisco, CA 94102.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- Calls would be received by customer service personnel and routed to SFPUC Emergency Planning and Security for additional follow up.

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.