Surveillance Technology Policy

Unmanned Aerial Vehicles ("UAV" or Drone technology)
Public Utilities Commission

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 ("UAV" 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

Our 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 ("UAV" 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 ("UAV" 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 ("UAV" or Drone technology) technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

- *Construction Management*: Examples include inspection of project sites for contract and environmental compliance.
- *Environmental Monitoring & Documentation*: Examples include monitoring of vegetation type and health, wildlife, and streams/reservoirs.
- *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.

Further, 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 for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

BUSINESS JUSTIFICATION

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

- The use of UAV's enables more efficient use of City resources and improved ability to inspect, manage and protect City infrastructure and natural resources.

In addition, Unmanned Aerial Vehicles ("UAV" or Drone technology) promises to benefit residents in the following ways:

- Education: Drone imagery to promote SFPUC projects and educate the public and on our mission and operations.
- Public Safety: Efficient inspection of critical infrastructure (dams, sewer infrastructure, power lines) helps ensure infrastructure is operating safely, minimizing overall risk of failure.

Unmanned Aerial Vehicles ("UAV" or Drone technology) will benefit the department in the following ways:

- 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.
- Time savings: Performing manual infrastructure inspections and environmental monitoring adds significant time to operations. See specific fountain thistle example above.
- 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)
- Improved data quality: Some locations which are difficult to access by personnel may be more easily photographed using drone technology, providing improved overall data.

To achieve its intended purpose, Drone or "UAV" technology utilizes an unmanned aircraft flown by a pilot via a ground control system, or autonomously through use of an on-board flight computer, communication links, or other any additional equipment, for the purpose of capturing images from an aerial perspective.

Department staff may use the technology for authorized use cases only, and is expressly prohibited from the following use cases:

SFPUC UAV operations will always be consistent with our approved use cases in SFPUC Drone Policy. 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.

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.

Each City drone must have a global positioning system.

Safety:

Surveillance technology must be operated in a safe manner. Drones may not have features (e.g., lights, coloring) or be used in a way that distracts drivers or other aircraft.

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 the following data types:

- Photographic and video data of assets, landscapes and property, JPEG, PNG, MOV, AVI, CSV (Level 2)
- License plate numbers, JPEG, PNG, MOV, AVI, SCV (Level 2)
- Faces/distinguishing features, JPWG, PNG, MOV, AVI, CSV (Level 2)

Notification:

Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. In addition, Departments shall notify the public of all drone flights by publishing flight summary data on the Open Data portal at least 24 hours in advance of operations. 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

Prohibited Zones:

Drones may not be used within five miles of an airport or in any FAA no-fly zone unless approved by the appropriate authority. City drone operations must comply with FAA rules.

Drones may not hover over trolley, streetcar, or light rail line wires, above rail, bus and parking control facility yards, unless authorized by the SFMTA.

Drones are not authorized within 500 feet of historical landmarks without authorization from building management or owners, except in cases where an emergency exists or FAA waiver is provided. San Francisco historical landmarks are defined by Article 10 of San Francisco's Planning Code. (e.g. City Hall, the Ferry Building. A full list is available here: https://sfplanning.org/preservation)

Drones may not fly over Port properties subject to the Maritime Transportation Security Act of 2002 without the permission of the Port and/or terminal operator. Port officials will provide City agencies with a list of regulated maritime facilities.

Access:

All parties requesting access must adhere to the following rules and processes:

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 ~~t~~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.

Access requirements vary by party:

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

Department shall maintain access logs for surveillance technology and all data collected, processed, and/or stored by the surveillance technology. The name of the person making the log entry should be recorded, along with the date and time.

B. Members of the public, including criminal defendants

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.

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 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)

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

The Department currently participates in the following sharing practices:

A. 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

Department shares the following data with the recipients:

Raw data for purpose of cleansing and processing only

Authorized contractors (SF Drone School)

Data sharing occurs at the following frequency: As needed

Data is disclosed pursuant to the following legal standard(s): Unaware of specific legal standard

Cleansing and processing data only

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

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.

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.

Current records shall be retained as follows: where retention period specified by law; where federal, state, or local law prescribes a definite period of time for retaining certain records, the SFPUC will retain the records for the period specified by law. Examples of records to be maintained for a specific period are Conflict of Interest Forms 700, which must be retained seven (7) years pursuant to Government Code 81009(e); Accident-Injury reports must be retained 5 years pursuant to 29 CFR 1404.6

Where no retention period specified by law, the SFPUC must specify the retention period for those records. Records shall be retained for a minimum of two (2) years, although such records may be treated as "storage records" and placed in storage at any time during the applicable retention period.

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.

SFPUC Records Management Policy

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:

- Local storage
- Department of Technology Data Center
- Software as a Service Product
- Cloud Storage Provider: Multivista Documentation Software (MDS) is a secure, cloud-based platform that stores all of the photos, videos, and drone-captured visuals.

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.

Drone operators must obtain remote pilot certifications from the FAA and must comply with all other FAA requirements

Contractors: If entering into a contract with a third party to operate drones, the contract should consider including the following requirements:

- The department shall require the contractor to comply with the department's approved drone policy which shall be attached to the contract and incorporated by reference.
- Ownership and handling of drone footage - "The Department of Public Works 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 Department of Public Works retains ownership and rights to Department Data, including derivative works made from Department Data and the licensing applied to the data. Contractors must treat Department 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.
- Data Security – Contractors must identify the application used to remove personal identifiable information that may have incidentally collected during an authorized flight.
- Insurance required – Contractor drone operators must provide proof of liability insurance commensurate with current SFPUC insurance requirements for contractors.
- Use Agreement Language - If an Unmanned Aircraft System (UAS) is used for any purpose under this permit either directly by the Contractor or by a subcontractor to the Contractor, the Contractor shall ensure that such activity is covered by Unmanned Aircraft Systems insurance. The Contractor must submit proof of UAS insurance with an aggregate limit of at least $2,000,000. The certificate of insurance must include a separate policy endorsement showing proof of UAS coverage which at a minimum shall include coverage for damage to person and property. A second (separate) endorsement must be submitted naming the City and County of San Francisco, its officers, agents and employees as Additional Insured for this coverage. NOTE: Each of these two endorsements require a separate attachment to the certificate of insurance.

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.

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

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.

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.

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 use of UAV's enables more efficient use of City resources and improved ability to inspect, manage and protect City infrastructure and natural resources.

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:

Construction Management: Examples include inspection of project sites for contract and environmental compliance.

Environmental Monitoring & Documentation: Examples include monitoring of vegetation type and health, wildlife, and streams/reservoirs.

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.

Rules:

SFPUC UAV operations will always be consistent with our approved use cases in SFPUC Drone Policy. 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.

Prohibited Uses:

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.

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

Photographic and video data of assets, landscapes and property

JPEG, PNG, MOV, AVI, CSV

License plate numbers

JPEG, PNG, MOV, AVI, SCV

Faces/distinguishing features

JPWG, PNG, MOV, AVI, CSV

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:

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.

Department:

San Francisco Public Utilities Commission: Construction Management Bureau

If applicable, contractor or vendor name:

SF Drone School

Rules and processes required prior to data access or use:

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 and the Drone Oversight Committee.

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

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.

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:

SFPUC Records Management Policy

Reason for retention:

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.

Deletion process:

SFPUC Records Management Policy

Retention exemption conditions:

All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.

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:

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.

How it can be accessed:

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:

Authorized contractors (SF Drone School)

Justification:

Unaware of a specific legal standard.

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

Description of training:

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.

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

Process for responding to complaints:

SFPUC Emergency Planning staff.

Oversight process:

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.”

Compliance personnel titles:

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

Restrictions:

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.

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:

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

Departmental follow-up process:

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.