Surveillance Technology Policy

Unmanned Aerial Vehicle (UAV) or Drone Technology

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 Vehicle (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

The Department's Mission is to provide innovative, reliable, and secure business solutions that support and empower CCSF agencies and departments in their delivery of high-quality government services for the public. The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned Aerial Vehicle (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 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 drone technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy. The Department is solely authorized to use drone technology to capture of video and still photographs as elements of the City video productions.

On an annual basis, the Department will evaluate the impact of the technology on the following measures: minutes of footage used in video productions.

BUSINESS JUSTIFICATION

Drone Technology supports the Department's mission and provides important operational value in the following ways: The Department of Technology's video channel SFGovTV provides the public critical information about government and civic life program through cable channels and web streaming. Drone technology will allow SFGovTV to produce improved video programming. Specifically, drone technology will allow the station to capture of video and still photographs as elements of the City video productions program.

In addition, drone technology promise to benefit residents by enhancing civic engagement SFGovTV's use of drone technology will allow residents to have an improved view of City operations and civic life.

To achieve its intended purpose, drone technology (or the "surveillance technology") incorporates unmanned, remotely-operated aircraft with onboard visual recording 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 using drone technology to intentionally capture images of a personal nature.

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 the following data types:

	Data Type	Formats	Classification
	Photographic and video data (no audio) of assets, landscapes, etc.	JPEG, PNG, MOV, AVI, CSV	Level 1
	Inadvertent capture of license plate numbers.	JPEG, PNG, MOV, AVI, CSV	Level 2
	Inadvertent capture of faces/distinguishing features	JPEG, PNG, MOV, AVI, CSV	Level 2
Notification:	Department includes the following items in its public notice: • Information on the surveillance technology • Description of the authorized use • Type of data collected • Department identification • Contact information		
Access:	The intent of SFGovTV is to provide information in the form of video programming to the public and city employees. Consequently, there are no special requirements for access to any of this information, including criminal defendants. Collected data that is classified as Level 1-Public data may be made available for public access or release via SFGovTV's video archive or 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. No outside vendors will be required to support and maintain the surveillance technology and its associated data. 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.		
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: only authorized drone operator(s) and General Manager may access unedited data.		

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 both internally and externally: Data sharing occurs at the following continuously Data is intended for public disclosure, so legal standard(s) for disclosure are not relevant. To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Scrub raw data collected by any drondes of any inadvertently collected PII as soon as possible and delete as soon as possible.
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: • Raw data collected by drones will be scrubbed of any inadvertently collected PII as soon as possible and deleted as soon as possible. • Programming using scrubbed data will be archived. • Programming is intended as an enduring record of city operations. PII data will typically not be collected. In cases where it is inadvertently collected, it shall immediately be scrubbed so that it will not permits identification of individuals. Raw data will be stored locally. Programming will be stored by cloud storage provider.
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 and use shall be explained in Departmental Drone Policy. All authorized users must sign off on policy prior to use.

COMPLIANCE

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

One individual with that has reviewed and signed the drone policy and received drone flight certification will be responsible for compliance with policies, procedures and record keeping.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties: General Manager, SFGTV.

Sanctions for violations of this Policy include the following:
First offense: violator shall be verbally notified by DT management of nature of violation. Second offense: violator shall notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days. Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from drone operations and disciplinary action may be taken depending upon the severity of second/third offences.

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 <u>not</u> 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 Members of the public can register complains, concerns or ask questions by calling (415) 554-4188 or send an e-mail to sfgovtv@sfgov.org.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall: SFGovTV will monitor drone program related complaints and respond within two business days.

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.

Drone technology incorporates unmanned, remotely-operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective.
There are no providers whose services are essential to the functioning or effectiveness of the drone technology.

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.

Drone Technology supports the Department's mission and provides important operational value in the following ways: The Department of Technology's video channel SFGovTV provides the public critical information about government and civic life program through cable channels and web streaming. Drone technology will allow SFGovTV to produce improved video programming. Specifically, drone technology will allow the station to capture of video and still photographs as elements of the City video productions program.

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.

The drone technology is authorized for Video Production, the apture of video and still photographs as elements of the City video productions.

Use of drone technology to intentionally capture images of a personal nature will always be prohibited.

Data must always be scrubbed of PII as stated above prior to use.

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

Data Type	Formats
Photographic and video data (no audio) of assets, landscapes, etc.	JPEG, PNG, MOV, AVI, CSV
Inadvertent capture of license plate numbers.	JPEG, PNG, MOV, AVI, CSV
Inadvertent capture of faces/distinguishing features	JPEG, 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: Video Programming Manager 1767

Only authorized drone operator(s) and General Manager may access unedited data.

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

Data must always be scrubbed of PII as stated above prior to use.

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

Programming using scrubbed data will be archived.
Programming is intended as an enduring record of city operations.
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

Raw data collected by drones will be scrubbed of any inadvertently collected PII as soon as possible and deleted as soon as possible.

Scrubbed data will be available through channels and web streaming.

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.

DT anticipates that video programming which includes video captured by drone will be publicly available through cable channels and web video streaming.

Scrubbed data will be integrated in video programming.

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

Drone data collection and use shall be explained in Departmental Drone Policy. All authorized users 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

Drone data collection and use shall be explained in Departmental Drone Policy. All authorized users must sign off on policy prior to use. The General Manager of SFGovTV will be assigned to ensure compliance. If the General Manager finds that the Drone Policy or this Surveillance Policy has not been followed, the following disciplinary measures will be taken:
First offense: violator shall be verbally notified by DT management of nature of violation.
Second offense: violator shall notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.
Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from drone operations and disciplinary action may be taken depending upon the severity of second/third offences.

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.

Complaints or concerns can be submitted to the Department by Members of the public can register complains, concerns or ask questions by calling (415) 554-4188 or send an e-mail to sfgovtv@sfgov.org.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall: SFGovTV will monitor drone program related complaints and respond within two business days.