Surveillance Technology Policy

UAV or Drone technology
San Francisco Fire Department

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 drones 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:

The mission of the Fire Department is to protect the lives and property of the people of San Francisco from fires, natural disasters, and hazardous materials incidents; to save lives by providing emergency medical services; to prevent fires through prevention and education programs; and to provide a work environment that values health, wellness and cultural diversity and is free of harassment and discrimination.

The Surveillance Technology Policy ("Policy") defines the manner in which the drones 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 drones, 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.

Authorized Use Case #1	*Disaster Response: Assessment and District Surveys*
Authorized Use Case #2	*Emergency Response: Building Fire Reconnaissance*
Authorized Use Case #3	*Search & Rescue: Aerial or water borne drones.*
Authorized Use Case #4	*Training: Assessment and evaluation of emergency response*

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

Drones support the Department's mission and provides important operational value in the following ways:

The mission of the SFFD UAS Program is to facilitate saving lives and property, enhance Firefighter safety and improve emergency response actions by providing aerial reconnaissance and observation to the Incident Commander to support strategic and tactical decisions at emergencies, major incidents and/or disasters. The SFFD will use uniformed personnel or an authorized contractor to operate the UAS.

In addition, drones promise to benefit residents in the following ways:

Education: drone imagery to promote Fire Department safety messaging and disaster preparedness

Environment: drone imagery to identify any hazardous material response and mitigation

Public Safety: emergency response as indicated in authorized use cases

Drones will benefit the department in the following ways:

Financial savings: drones can be far more time efficient and cost effective when conducting emergency response and gaining rapid situational awareness in a disaster.

Time savings: deploying a drone can provide time savings locating victims in a variety of environments as well as gain situational awareness and hazard assessment.

Staff safety: drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.

Improved data quality: some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

To achieve its intended purpose, drone 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 the following use cases:

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

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: Each City drone must have a global positioning system. ~~Each C~~The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

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:

Data Type(s)	**Format(s)**	**Classification**
Photographic and video data (no audio) of assets, landscapes, etc.	*JPEG, PNG, MOV, AVI, CSV*	Level 2
License plate numbers	*JPEG, PNG, MOV, AVI, CSV*	Level 2
Faces/distinguishing features	*JPEG, PNG, MOV, AVI, CSV*	Level 2

Notification: Where feasible, 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 of such collection.

Where feasible, 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.

Operators may wear special safety vests with language to identify their status as drone pilots. Notice will be made to the Department of Emergency Communications, in addition to the required notifications per City use policy.

For disaster/emergency response advance notice may be unlikely. If a DOC is mobilized in anticipation of an emergency event, flight details may potentially be announced through the PIO in addition to the required notifications per City use policy.

Department includes the following items in its public notice:

- Information on the surveillance
- Description of the authorized use
- Type of data collected
- Will persons will be individually identified
- Data retention
- Department identification
- Contact information

Prohibited Zones: During emergency operations in which drone operation is critical to life safety, life saving, hazard mitigation, or property protection, pursuant to an approved FAA 107 exemption and COA waiver approval, the SFFD will be exempt from the requirement to provide prior notification of UAS operation to the Port, MTA, and historic building owners.

Pursuant to valid FAA 107 exemption and COA waiver approvals, SFFD shall where necessary for an emergency response engage in UAS operations that may involve: flight over people, night operations, maximum altitude restrictions, visual line of sight, and airport restrictions. Each of these waivers is incorporated by reference herein.

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

Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

Data access and use are restricted to

Only authorized drone operators or MIS may access unedited data.

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.

- Drone Program Manager

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

- It is possible drone contractors may be retained as part of a professional services contract.

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 be made available to members of the public, including criminal defendants. Data can be accessed by the public in the following ways: Only data with no PII may be accessible or available for use by the public, including criminal defendants. No unedited data will be accessed by 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:

Only authorized drone operators or MIS 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:

A. Internal Data Sharing

Department shares the following data with the recipients:

It is possible other departments may request to review edited images (scrubbed of "PII").

Data sharing occurs at the following frequency:

Uncertain - will vary by case.

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

We are unaware of a specific legal standard in this regard. However, as responsible service providers the Fire Department believes in granting appropriate requests. Such a disclosure would be made in the best interests of our partner agencies as allowable by the data sharing policy.

B. External Data Sharing

The SFFD Compliance Officer will review all data or imagery prior to release for public information requests or for official SFFD business purposes. MIS staff and the SFFD Compliance Officer will be trained in all applicable SFFD and City and County of San Francisco Drone and Data Retention Policies.

The SFFD UAS shall not be operated to obtain data for law enforcement purposes unless legally required to do so. Stored data that includes PII shall not be shared with or disseminated to law enforcement or any other person or entity unless legally required to do so.

Acquisition, transfer and dissemination of data and imagery shall be documented in the SFFD UAS logbook and all other records required by local, state or federal law.

No personal use or sharing of UAS data and imagery is allowed. SFFD members will not store, transfer or utilize SFFD electronic data or imagery for personal use. SFFD members will not post, transmit, store or otherwise disseminate confidential or sensitive information including data, imagery, or sound relating to work assignments without the express permission of the Chief of Department or his/her designee.

Requests for copies of the stored data and imagery shall require a written request from the requestor, per the City and County of San Francisco Public Information Request Policy and will be reviewed prior to release by SFFD MIS staff and the SFFD

Compliance Officer and/or the City and County of San Francisco Attorney General's Office.

Copies of SFFD data and imagery will not be made available unless the person requesting the copy is authorized to view the recording and does not otherwise have access to the SFFD data and imagery. This may include public information requests after the recordings have been reviewed and redacted by the SFFD.

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

Fire Department policy will prevent sharing data with any entities data that has not been edited to remove PII.

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:

The Fire Department will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-processed (i.e., "scrubbed") data will be maintained by the Fire Department per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.	Scrubbed data will adhere to the SFFD 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 will not be retained beyond the standard retention period.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

Local storage
Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card). Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Fire Department servers by Drone Data Editor. The Fire Department Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain. Once the subject image frames, still and/or video, have been identified for business needs, the Fire Department Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain. After processing and saving of edited data, all raw data will be permanently erased. Before replacing the SD storage cards into the drone, data editor will ensure the discs are completely free of all data. 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.

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

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.

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 - "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.
- 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:

Drone Operators will be assigned to maintain updates and perform required maintenance. A procedural pre-mobilization and post-mobilization safety check will be performed at each operation.

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

Supervisor- Management of Information Services

Sanctions for violations of this Policy include the following:

First offense: violator shall be verbally notified by Fire Department management of nature of violation.

Second offense: violator shall be 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.

ROLES AND RESPONSIBILITIES

1. Departments participating in the drone evaluation years are required to adopt a policy that reflects the requirements iterated in this document. The departmental drone policy must be reviewed and signed by all drone operators in participating departments, and any individuals with access to drone data that may contain Personal Identifiable Information.

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

Members of the public can register complaints / concerns or submit questions through the Fire Department website and complaint process.

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

Constituent calls and complaints to the Fire Department are routed to the Drone Program manager. Program manager will discuss concerns or complaints with constituent and record details regarding nature of conversation. If additional action is required or requested by caller, the Fire Department commits to a follow-up (by email or telephone) in a timely manner.

UAS Program Manager, drone operators, and Fire Department management shall review log on a quarterly basis to discuss best practices, evaluate for learning lessons and opportunities to improve and refine the drone use program based on caller complaints, concerns and other community feedback.

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. *DJI Matrice 210 is an aerial survey drone: "SEARCH AND RESCUE"* *Equipped with both an aerial zoom and thermal camera, first responders can now quickly locate missing people in remote areas and plan the safest approach path"* *Uncertain at this time.*
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 will support our mission through the following: The mission of the SFFD UAS Program is to facilitate saving lives and property, enhance Firefighter safety and improve emergency response actions by providing aerial reconnaissance and observation to the Incident Commander to support strategic and tactical decisions at emergencies, major incidents and/or disasters. The SFFD will use uniformed personnel or an authorized contractor to operate the UAS. Photographic and video data (no audio) of assets, landscapes, etc. License plate numbers Faces/distinguishing features
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.
Disaster Response: Assessment and District Surveys *Emergency Response: Building Fire Reconnaissance* *Search & Rescue: Aerial or water borne drones.* *Training: Assessment and evaluation of emergency response*

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

Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

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

Data Type(s)	**Format(s)**	**Classification**
Photographic and video data (no audio) of assets, landscapes, etc.	*JPEG, PNG, MOV, AVI, CSV*	Level 2
License plate numbers	*JPEG, PNG, MOV, AVI, CSV*	Level 2
Faces/distinguishing features	*JPEG, PNG, MOV, AVI, CSV*	Level 2

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.

Drone Program Manager

Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

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

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

Only authorized drone operators or MIS may access unedited data.

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

The Fire Department will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-processed (i.e., "scrubbed") data will be maintained by the Fire Department per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.

Scrubbed data will adhere to the SFFD Records Management Policy

Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card). Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Fire Department servers by Drone Data Editor. The Fire Department Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain. Once the subject image frames, still and/or video, have been identified for business needs, the Fire Department Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain. After processing and saving of edited data, all raw data will be permanently erased. Before replacing the SD storage cards into the drone, data editor will ensure the discs are completely free of all data.

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

Only data with no PII may be accessible or available for use by the public, including criminal defendants.

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.

The SFFD Compliance Officer will review all data or imagery prior to release for public information requests or for official SFFD business purposes. MIS staff and the SFFD Compliance Officer will be trained in all applicable SFFD and City and County of San Francisco Drone and Data Retention Policies.

The SFFD UAS shall not be operated to obtain data for law enforcement purposes unless legally required to do so. Stored data that includes PII shall not be shared with or disseminated to law enforcement or any other person or entity unless legally required to do so.

Acquisition, transfer and dissemination of data and imagery shall be documented in the SFFD UAS logbook and all other records required by local, state or federal law.

No personal use or sharing of UAS data and imagery is allowed. SFFD members will not store, transfer or utilize SFFD electronic data or imagery for personal use. SFFD members will not post, transmit, store or otherwise disseminate confidential or sensitive information including data,

imagery, or sound relating to work assignments without the express permission of the Chief of Department or his/her designee.

Requests for copies of the stored data and imagery shall require a written request from the requestor, per the City and County of San Francisco Public Information Request Policy and will be reviewed prior to release by SFFD MIS staff and the SFFD Compliance Officer and/or the City and County of San Francisco Attorney General's Office.

Copies of SFFD data and imagery will not be made available unless the person requesting the copy is authorized to view the recording and does not otherwise have access to the SFFD data and imagery. This may include public information requests after the recordings have been reviewed and redacted by the SFFD.

It is possible other departments may request to review edited images (scrubbed of "PII").

All CCSF Departments may make a request and will be granted on a case by case basis.

Uncertain - will vary by case.

Images of assets (with PII removed or obscured)

We are unaware of a specific legal standard in this regard. However, as responsible service providers the Fire Department believes in granting appropriate requests.

Such a disclosure would be made in the best interests of our partner agencies as allowable by the data sharing policy.

Fire Department policy will prevent sharing data with any entities data that has not been edited to remove PII .

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

Fire Department policy will prevent sharing data with any entities data that has not been edited to remove PII .

Drone Operators will be assigned to maintain updates and perform required maintenance. A procedural pre-mobilization and post-mobilization safety check will be performed at each operation.

Supervisor- Management of Information Services

***First offense**: violator shall be verbally notified by Fire Department 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.*

Only authorized drone operators or MIS may access unedited data.

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.

Members of the public can register complaints / concerns or submit questions through the Fire Department website and complaint process.

Constituent calls and complaints to the Fire Department are routed to the Drone Program manager. Program manager will discuss concerns or complaints with constituent and record details regarding nature of conversation. If additional action is required or requested by caller, the Fire Department commits to a follow-up (by email or telephone) in a timely manner.