



CCSF UNMANNED AIRCRAFT SYSTEM (DRONE TECHNOLOGY) POLICY

Committee on Information Technology (COIT)

The City and County of San Francisco (“City”) recognizes the potential of Unmanned Aircraft Systems (UAS), colloquially known as drones, to improve service delivery, support public safety, enhance emergency response, and expand the City’s overall capacity to meet community needs. As the use of UAS is expected to grow across departments, the City is committed to maximizing public benefit while minimizing potential harms to privacy, safety, and community trust.

PURPOSE AND SCOPE

The purpose of this Unmanned Aircraft System Policy (“Policy”) is to establish technical and operational standards for the coordinated, safe, and accountable acquisition and use of Unmanned Aircraft System (“UAS”) by City departments, as well as the efficient, secure, and responsible handling and sharing of the data collected by a UAS. It establishes a unified framework for all departments to prevent operational fragmentation and inconsistent practices that could create safety hazards, inefficient resource allocation, or coordination failures, especially during multi-agency responses.

This Policy applies to all UAS operations conducted by, for, or on behalf of the City, including all City Departments, boards, commissions, and affiliated agencies, as well as City employees, contractors, consultants, volunteers, and vendors involved in any City-approved UAS program.

This Policy also applies to third-party operators conducting drone services under City contracts or permits and City-authorized programs involving coordinated multi-aircraft operations and other public-facing activities.

The Policy applies to all UAS operations within City jurisdiction. The jurisdictional boundaries include all operations within the City’s geographic boundaries, operations originating from City facilities or conducted by City personnel outside jurisdictional boundaries, and regional mutual aid operations where City personnel or equipment are deployed.

The temporal scope governs all UAS operations from the effective date forward, with existing UAS programs required to achieve compliance within 180 days of this Policy’s adoption.

POLICY STATEMENT

The City establishes this UAS Policy to ensure the responsible deployment of UAS technology in service of the public good. The City recognizes that UAS technology offers significant opportunities to enhance municipal services, improve emergency response capabilities, and increase operational efficiency, while simultaneously acknowledging that these same capabilities require careful governance to protect fundamental rights, protect the safety of persons and property, and maintain community trust.

This policy reflects San Francisco's commitment to using UAS in ways that uphold the City’s values of transparency, accountability, privacy protection, and community engagement. UAS

COIT Policy Dates

Approved:

technology offers an efficient, economical, and impactful means of providing vital real-time information for addressing emergencies, public safety and infrastructure needs, but only when deployed with appropriate safeguards and oversight.

Through this Policy, the City establishes a unified framework that:

- **Maximizes public benefit** through coordinated UAS efforts that ensure the efficient and effective use of City resources;
- **Protects constitutional rights** by maintaining robust safeguards for privacy, civil liberties, and due process protections, particularly for vulnerable people and marginalized communities;
- **Ensures due diligence** by establishing technical and safety standards that minimize risks while enabling effective mission accomplishment;
- **Promotes accountability** by creating transparent governance structures with clear oversight mechanisms and public disclosure;
- **Enables future innovation** by establishing the foundation for a scalable, interoperable UAS infrastructure.

Department policies must be consistent with this Policy and must comply with the Municipal Charter and all applicable City, State, and Federal laws and regulations--including current and future Federal Aviation Administration (FAA) rules governing UAS--, as well as all state and federal Constitutional guarantees. In the event of any conflict between this Policy and applicable federal or state law, Federal Aviation Administration (FAA) requirements, the terms of any Certificate of Authorization (COA), Certificate of Waiver (COW), or other approved waiver, operators shall comply with the controlling law, requirement, or authorization. To the extent permitted by law, any requirements or approvals issued by an authorized oversight body for the Department's UAS operations shall also control in the event of a conflict with this Policy.

Nothing in this Policy shall prohibit the use of drones or UASs by any law enforcement agency for lawful purposes and in a lawful manner.

Departments whose UAS operations are governed by a Board-approved Surveillance Technology Policy in accordance with San Francisco Administrative Code Chapter 19B are exempt from drafting and maintaining a separate Departmental UAS Policy, provided that the relevant Surveillance Technology Policy—and any associated procedures, procurement specification, and contract terms—collectively implement the policy requirements outlined in this Policy. A department relying on a Board-approved Chapter 19B Surveillance Technology Policy may satisfy the “policy requirements outlined in this Policy” through a combination of (i) its 19B Surveillance Technology Policy and internal operating procedures, (ii) procurement specifications and solicitations that require compliance with this Policy’s “Specifications” requirements, and (iii) contract terms that require compliance with this Policy’s “Third-Party UAS Providers, Contractors, and Vendors” requirements. Procurement and contracting requirements in this Policy need not be duplicated in the department’s 19B policy or a separate Departmental UAS Policy solely for that purpose.

POLICY REQUIREMENTS

Specifications

Each UAS considered for procurement or operational use must comply with all applicable FAA regulations, complete the Department of Technology Chief Information Officer (CIO) Review

process, and possess the technical capabilities necessary to support safe, reliable, and secure operations within the City. At minimum, each aircraft must include:

- A positioning and navigation capability (e.g., GPS and/or alternative system such as inertial and/or vision-based navigation) to support safe navigation and return-to-home functionality;
- Up-to-date software and/or firmware for the aircraft and control system [14 CFR §107.15 and §107.49];
- Active FAA registration; the FAA registration number must be clearly marked on the exterior, as applicable under federal requirements;
- Remote ID capability (i.e., a “digital license plate”), where required under applicable FAA rules [14 CFR Part 89];
- Collision and obstacle avoidance technology sufficient to support safe operation in urban and congested environments;
- Anti-collision lighting visible for at least 3 statute miles when operating at night or during civil twilight [14 CFR § 107.29].

Safety

Each department operating a UAS program must establish, maintain, and adhere to Safety Protocols that are appropriate to its mission, compliant with all applicable FAA regulations, and consistent with the guidance provided in Annex A. These Safety Protocols must be formally documented, kept up to date, and accessible to all personnel involved in UAS activities. All such personnel must review and acknowledge the department’s Safety Protocols in writing as a condition of participating in UAS operations. At minimum, each department’s Safety Protocols must address:

- Pre-flight safety procedures, including aircraft readiness, environmental and airspace assessment, and mission authorization requirements;
- In-flight safety procedures, including crew roles, responsibilities, and procedures for abnormal or unsafe conditions;
- Operating limitations and flight rules;
- Incident reporting and corrective actions, including immediate reporting, documentation, internal review, and follow-up measures. For law enforcement operations, reporting timeliness may be adjusted to reflect operational tempo and safety considerations;
- Preventive maintenance and equipment inspections, including schedules and record-keeping.

Training

To ensure safe, legal, and consistent drone operations across all City departments, UAS program staff shall meet and maintain minimum training requirements. These requirements must reflect FAA regulations, NIST’s test methods for small UAS (sUAS), as well as additional City-specific requirements to support the City’s commitment to public safety, accountability, and operational readiness.

Remote Pilots in Command (RPIC) must:

- Hold a current FAA Part 107 Remote Pilot Certificate;
- Obtain written authorization from the responsible UAS Program Manager;
- Participate in department-level training programs whenever available.

Visual Observers (VO) must:

- Complete role-appropriate training on communications, situational awareness, and safety procedures;
- If supporting UAS night operations, complete training that addresses visual illusions and sensory limitations encountered in darkness and demonstrates mitigation strategies;
- Participate in department-level training programs whenever available.

City Departments deploying UAS must:

- Ensure all UAS operators hold a valid FAA Remote Pilot Certificate or meet the pilot-qualification standards spelled out in the department's FAA-issued COA;
- Ensure that authorized visual observers of UAVs have completed sufficient training to communicate to the pilot any instructions required to remain clear of conflicting traffic. This training, at minimum, shall include knowledge of the rules and responsibilities per FAA guidelines/COA duties;
- Unless existing departmental programs already provide it, and as resources allow, provide training and mental health support for staff, including dispatchers and public safety personnel, who may be exposed to graphic or traumatic drone footage, to reduce the risk of vicarious trauma and secondary stress injuries;
- Evaluate the flight skills and proficiency of drone operators at least once every 24 months based on NIST's standards, with more frequent evaluations recommended for UAS operators involved in public safety and emergency response missions given their higher risk;
- Retain training and proficiency records for both UAS operators and visual observers for a minimum of two years from last date of completions.

Public Transparency

Departments deploying UAS shall provide clear, accessible public information on the Department's website or the City's Open Data Portal, including:

- The permitted use cases, prohibitions, and restrictions, as set forth in the department's policy or ordinance for the technology;
- The program scope, objectives, public benefits, and governing policies of the UAS program;
- The categories of data UASs may capture, along with the procedures for data maintenance, storage, access, sharing (within and outside of the jurisdiction), and disposal;
- The measures in place to safeguard individual privacy, civil liberties, and constitutional rights of City residents and visitors;
- An updated set of FAQs about the department's UAS program;
- A monthly flight log with flight summary information, mission purpose, and the type of data collected, except where disclosure would compromise operational security or safety. Departments must also maintain an internal record of names of assigned staff for each flight to support incident investigation and corrective actions, internal audits, public records requests, and legal holds.

Prohibited Zones

City UAS operations are prohibited in any location where federal, state, or local rules restrict or forbid unmanned aircraft operations unless the department has obtained the required authorization or waiver. To ensure public safety and avoid interference with manned aircraft or critical infrastructure, the remote pilot in command (RPIC) must verify all applicable airspace restrictions before each flight and remain logged into an approved real-time airspace awareness system during operations. Where feasible for routine, non-emergency operations, departments should enable UAS geofencing features to prevent entry into restricted or prohibited airspace.

A non-exhaustive list of no-fly zones and restricted areas in the City is provided in Annex B.

Privacy

In order to collect data using a UAS, Departments need a list of authorized use cases and to operate the UAS according to the terms of one of those authorized use cases.

Departments should minimize the collection, use, and retention of personally identifiable information (PII) to what is strictly necessary to accomplish the intended purpose of each UAS operation. Should PII be incidentally captured, departments must remove or irreversibly de-identify that data before public release or sharing, unless required for a public safety purpose.

UAS operators must not intentionally record or transmit images of places where people have a reasonable expectation of privacy (such as inside homes, fenced yards, or other private areas), except when authorized by a valid warrant or when otherwise permitted by law. Whenever operationally feasible, operators must take reasonable steps to prevent inadvertent capture of such areas, including—but not limited to—turning off or disabling cameras not needed for aerial safety, using geofencing overlays to restrict flight paths, or adjusting the flight altitude, angle, or trajectory. This requirement does not apply when such capture is necessary to safely accomplish the mission. Additionally, departments should consider if the same operational goal can be achieved using privacy-enhancing technologies that reduce or eliminate the collection, retention, or use of PII.

These privacy-protective practices must be clearly documented in the Department's UAS Policy (or equivalent 19B Surveillance Technology Policy) and integrated into UAS training programs and standard operating procedures.

Data Governance

Departments' UAS data governance protocols must be consistent with the City's Data Management Policy, Data Classifications Standards, other applicable laws, as well as with the following Citywide standards.

A. Classification

All UAS-collected data must be classified according to the City's Data Classification Standards, and metadata recorded in the annual Data Systems and Dataset Inventories, in accordance with Administrative Code Chapter 22D and Chief Data Officer (CDO) guidance.

Departments must follow the City's Data Standards Guide when classifying and labeling UAS-generated data.

B. Access

Access to UAS data must be limited to trained City staff with a documented operational need. Each department must:

- Designate a Data Steward responsible for day-to-day data governance;
- Assign a Privacy Officer to oversee compliance with privacy laws and coordinate with the CDO and Department of Technology (DT) as needed.

C. Storage

Any UAS data that is retained must be stored in a secure local or City-approved cloud system that satisfies the cybersecurity requirements set forth in the City's Data Management Policy.

D. Retention

Departments' UAS data retention policies must be consistent with Administrative Code Chapter 8 and any other applicable retention schedules and legal requirements. PII must be retained only as long as necessary, and they must be access-controlled at all times.

Departments must implement automated deletion protocols and conduct quarterly audits of retention compliance.

E. Sharing

UAS data sharing must comply with the City's Data Management Policy and any applicable approved Surveillance Technology Policy.

Departments should avoid replicating full datasets and, whenever feasible, provide secure access rather than transferring copies. Privacy & Security Toolkits must be applied when sharing non-public data.

During exigent circumstances or declared emergencies, departments may share raw or live drone footage with other City departments to support public safety, emergency management, or disaster response operations. Post-emergency, all retained data must comply with standard retention, minimization, and deletion requirements.

External sharing is prohibited unless required by law or expressly authorized under a written data-sharing agreement approved through the City's standard review process. Any disclosure must be limited to the minimum necessary and documented. For public safety operations, sharing with external third parties is permitted to the extent required to successfully complete the mission. Nothing in this policy restricts disclosures required by law, which must follow the City's standard legal review and disclosure procedures, or authorized community relations and engagement activities.

Emergency UAS Coordination and Information Sharing

When the Emergency Operation Center (EOC) is activated, all UAS requests should follow the Incident Command System (ICS) structure and the EOCs established coordination processes. While public safety and law enforcement departments should continue to use their discipline-specific mutual-aid channels to obtain UAS resources, the EOC should be notified to ensure situational awareness and integration into the common operating picture.

Departments may view or request live UAS footage, as appropriate, through the EOCs established information-sharing protocols or direct coordination with the operating department.

Airspace Awareness and Security

Detecting UAS activity and reporting unauthorized UAS supports public safety by promoting safe operations and enabling timely response to potential security threats. City Departments engaged in UAS operations must participate in City-approved detection-and-reporting systems as they are developed. Counter-UAS measures are generally prohibited unless carried out under the documented authority of federal or other legally authorized entity.

UTM Integration

As City departments expand their use of UAS and the forecasted expansion of commercial UAS activity, the City anticipates the need for a coordinated UAS Traffic Management (UTM) framework that will support safe flight authorization and airspace deconfliction. A City-operated UTM system that meets federal standards would ensure interoperability and public transparency on airspace usage.

The Drone Advisory Committee will monitor federal UTM developments, evaluate operational and technical requirements, and coordinate planning across departments to ensure that emerging City detection and airspace-awareness systems are deployed in ways that can support future integration into a City-operated UTM system.

Third-Party UAS Providers, Contractors, and Vendors

Departments entering into agreements with external entities that provide UAS-related services (e.g., aerial inspections, public demonstrations, or one-time data collection) must ensure the following:

- Contracts must require third-party UAS service providers to comply with this Policy and the department's approved UAS policy, which shall be attached to the contract and incorporated by reference.
- Unauthorized UAS use or activities inconsistent with this Policy are strictly prohibited and may result in contract termination, fines, and other applicable penalties.
- Contractors must identify and document the tools or methods used to remove personally identifiable information (PII) that may be incidentally collected during authorized flights.
- Contractors must provide proof of UAS liability insurance with an aggregate limit of at least \$2,000,000. The certificate of insurance must include:
 - A separate endorsement for UAS coverage, including damage to persons and property; and
 - A separate endorsement naming the City and County of San Francisco, its officers, agents, and employees as Additional Insured.

For contractors embedded within City departments or engaged in ongoing drone-related work, the following requirements shall apply:

- Contract personnel operating UAS must hold a valid FAA Part 107 Remote Pilot Certificate or meet equivalent COA standards. They must also complete department-

specific training, maintain aeronautical knowledge currency, and comply with all City training requirements.

- Contractors must maintain logs of UAS operations, training records, incident reports, and data governance activities in alignment with CCSF standards, and must provide such records to the City upon request for audit or review.
- Contractors providing maintenance or repair services must document all work performed and adhere to the City's preventive maintenance policies and retention schedules.

Departments purchasing or leasing UAS hardware, software, or related equipment from a vendor must ensure that procurement contracts include the following:

- A certification that all UAS, equipment, and services provided are designed to meet FAA requirements and are capable of operating in compliance with departmental COAs and this Policy.
- Clear warranties and service-level agreements that ensure the safety, privacy, and cybersecurity of the equipment or service throughout its lifecycle.
- Vendors providing maintenance or repair services must document all work performed and adhere to the City's preventive maintenance policies and retention schedules.

In addition, all data collected, processed, stored or generated through UAS operations performed by third-party UAS providers, contractors or subcontractors on the City's behalf, or through vendor-provided UAS hardware, software, or cloud services, is considered "City Data." The City retains full ownership of City Data, including derivative works and licensing rights. Third-party UAS providers, contractors, subcontractors and vendors must protect and manage City Data in accordance with CCSF privacy and data security standards, as well as with the City's Data Management Policy.

ROLES AND RESPONSIBILITIES

City Chief Information Officer (CIO)

The City CIO is responsible for the following:

- Provide Citywide leadership by convening and directing the Drone Advisory Committee's work;
- Coordinate and support shared UAS technology services, including the data management platforms, communication systems, and interoperable technologies necessary to support safe, secure, and coordinated UAS operations across departments;
- Provide guidance to departments seeking to procure or use UAS, including support for shared contracts and DT-managed UAS resources to ensure interoperability, achieve economies of scale, and preserve the integrity of City technology environments;
- Support public safety departments and the Department of Emergency Management (DEM) by providing secure, resilient technology infrastructure for UAS use during emergencies and major incidents;
- Direct the City Chief Information Security Officer (CISO) to establish and maintain a registry of City-owned or City-operated UAS.

City Departments

For departments that operate a UAS Program, department leadership and program management are responsible for the following:

- Designate a UAS Program Manager;
- Designate a department representative and an alternate to the Drone Advisory Committee;
- Adopt and maintain a department-specific UAS policy and protocols that are consistent with this Policy;
- Ensure all UAS operators and any personnel with access to UAS-derived data complete required training, sign acknowledgements of the departmental UAS policy, and comply with all federal, state, and local laws;
- When using shared or pooled UAS assets, document procedures for equipment custody and access, flight scheduling and approval, routine inspections and maintenance, and any other processes needed for the safe, compliant, and accountable use of UAS equipment.

Department UAS Program Manager

Department UAS Program Managers are the accountable UAS Program leads and are responsible for the following, with support from designated staff as needed and in alignment with existing job classifications and duty statements:

- Ensure compliance with all applicable federal, state, and local laws;
- Establish and maintain the department's UAS policy and operational protocols;
- Maintain the department's UAS records, including training documentation, flight logs, inventories, authorizations, and compliance documents;
- Facilitate coordination, information-sharing, and collaboration with other City departments operating UAS programs through the Drone Advisory Committee.

Remote Pilots in Command (RPIC)

RPICs are responsible for the following:

- Comply with FAA rules, applicable departmental policies, as well as safety protocols;
- Maintain a valid FAA Part 107 Remote Pilot Certificate, including compliance with FAA recurrent training requirements and currency standards, and participate in departmental training.

Visual Observers (VOs)

VOs are responsible for the following:

- Comply with FAA rules, applicable departmental policies, as well as safety protocols;
- Complete role-appropriate training on communications, situational awareness, and safety procedures, including night operations training.

Drone Advisory Committee (“Committee”)

The Drone Advisory Committee is responsible for the following:

- Periodically review and evaluate this Policy and provide recommendations to COIT on revisions needed to reflect the latest UAS technological and regulatory developments;
- Promote, to the extent feasible, coordination on UAS acquisition, shared infrastructure, and interoperable systems across City departments;
- Monitor and advise departments on Citywide UAS airspace awareness and security efforts, including detection, information-sharing, and preparation for future UAS Traffic Management (UTM) capabilities.

QUESTIONS

All questions regarding this policy should be directed to the employee's supervisor or to the department director. Similarly, questions about other applicable laws governing the use of UAS or the issues related to privacy should be directed to the employee's supervisor or the director, although the supervisor or director may determine that the question must be addressed to the Committee on Information and Technology (COIT). Employees may also contact their unions for advice or information about their rights and responsibilities under these and other laws.

REFERENCES

The FAA has developed regulations on the use of unmanned aerial systems and drones. For more information, please refer to their website at: <https://www.faa.gov/uas/>

Other federal codes and laws apply to the use of drones, some of which are mentioned in this policy and listed below:

- [14 CFR Part 89](#)
- [14 CFR Part 107](#)
- [14 CFR 107.09](#)
- [14 CFR 107.15](#)
- [14 CFR 107.23](#)
- [14 CFR 107.29](#)
- [14 CFR 107.31](#)
- [14 CFR 107.33](#)
- [14 CFR 107.39](#)
- [14 CFR 107.49](#)
- [14 CFR 107.51](#)
- [14 CFR 107.65](#)
- [14 CFR 107.145](#)
- [Maritime Transportation Security Act of 2002](#)

This is a list of all local City and County of San Francisco laws that are relevant to drone usage and referenced earlier in this policy:

- [Administrative Code Chapter 8](#)
- [Administrative Code Chapter 12](#)
- [Administrative Code Chapter 12H](#)
- [Administrative Code Chapter 19B](#)
- [Administrative Code Chapter 22D](#)
- [Data Classification Standards](#)
- [Data Management Policy](#)

The policy also references best practices as outlined by federal guidelines— here are those guidelines:

- [NIST test methods for small unmanned aerial systems](#)

Note about References

The items in the reference section are meant to help departments understand the legal landscape surrounding UAS and drones that exists when this policy was last updated. Please consult with

your department's City Attorney before implementing a UAS/drone program for your department, as well as regularly after implementing a UAS/drone program, to ensure that your department is up to date with the current legal landscape and is abiding by all relevant local, state, and federal laws.

DEFINITIONS

Aeronautical knowledge currency Up-to-date knowledge of the principles, regulations, and procedures required to operate an unmanned aircraft (UA) on behalf of the City. For operators of small unmanned aircraft systems (sUAS) under Part 107, maintaining aeronautical knowledge currency involves recurrent training.

Beyond Visual Line of Sight (BVLOS) A broad spread of existing and potential UAS operations whose only common factor is the Uncrewed Aircraft (UA) being out of the direct visual line of sight of the remote pilot.

Certificate of Authorization (COA) This is an authorization given to government and public safety agencies to be able to self-certify UAS and operators for flights performing governmental functions. If the department does not have a COA they may operate under a 14 CFR part 107 (below 400 feet and visual line-of sight operations only).

As best practice, prior to usage of a UAS all government agencies, including law enforcement, flying a UAS for commercial purposes under part 107, shall register the specific UAS and all intended uses with the FAA and obtain a Certificate of Authorization (COA) authorizing them to use a UAS within a certain area of space, to be determined by the FAA in consultation with the applying agency. In an emergency, as described below, an Emergency or Special Government Interest COA will be issued.

City The City and County of San Francisco.

City Data All data that the City and County of San Francisco (City) collects, uses, maintains, processes, stores, or generates, including data arising from unmanned aircraft (UA) operations conducted by or for any City department, board, commission, or affiliated agency, and by City employees, contractors, consultants, volunteers, or vendors under any City-approved program, contract, permit, or authorization.

City Department or Department Any City official, department, board, commission, or other entity in the City.

Civil Twilight The time that begins in the morning, or ends in the evening, when the geometric center of the sun is 6 degrees below the horizon.

Class B / Class C / Class D airspace	Controlled airspace around busy (B), medium/large (C), and towered (D) airports, respectively, as designated in 14 CFR Part 71 and depicted on FAA aeronautical charts. Operators should confirm airspace class and applicable UAS restrictions/authorization using FAA charting and FAA-provided mapping tools or other UAS planning applications as appropriate.
Class E airspace	Controlled airspace that begins at ground level within the published lateral boundaries around an airport to contain instrument flight procedures.
Controlled airspace	The umbrella term for Class A, B, C, D, and E airspace where ATC services are provided.
Data Steward	Refer to the City's Data Management Policy for the official definition and responsibilities of the Data Steward role.
Deconfliction (of a flight path)	The process of adjusting or coordinating the paths of two or more aircraft to avoid a collision or a "near-midair" collision.
Drone as First Responder (DFR)	A model in which prepositioned unmanned aircrafts (UA) at fixed launch sites are remotely dispatched to incidents, often preceding ground units, providing real-time video and sensor feeds to dispatchers and responders to enhance situational awareness, reduce response times, and improve safety and decisions during collisions, calls for service, crimes in progress, search operations, and other law enforcement activities, including criminal investigations and general police work.
Drone Data	All information collected or generated by an unmanned aircraft system and derived products (e.g., photos, videos, audio, Light Detection and Ranging (LiDAR), thermal data) and associated metadata (e.g., geolocation, time, altitude, heading, sensor settings). The term "raw" Drone Data refers to Drone Data that has <u>not</u> been processed and cleaned of all personal identifiable information. The distribution and use of raw drone data is tightly restricted.
Emergency operations	Coordinated responses to natural disasters, major incidents, or declared emergencies.
Exigent circumstances	A situation requiring immediate action where delaying to obtain the required authorization would be impracticable and would risk imminent danger of death or serious physical injury to any person; the imminent escape of a suspect; or the imminent destruction of evidence.
Federal Aviation Administration (FAA)	A Federal agency within the US Department of Transportation that regulates civil aviation, including unmanned aircraft systems.

National Institute of Standards and Technology (NIST)	A nonregulatory Federal agency within the US Department of Commerce that promotes innovation and industrial competitiveness of the United States of America by advancing measurement in science, standards, and technology.
Notice to Airmen (NOTAM)	An official, time-critical aeronautical notice that alerts those involved in flight operations to temporary or abnormal changes to facilities, services, procedures, or hazards—information not known far enough in advance to publish by other means. Examples include runway closures, navaid outages, and temporary airspace restrictions. NOTAM procedures and points of contact vary by operation type, and City departments should coordinate with the FAA and/or the appropriate air traffic authority to determine whether a NOTAM, TFR, or another notification/authorization process applies.
Part 107	Part 107 is a set of rules issued by the Federal Aviation Administration (FAA) governing civil operations of small unmanned aircraft systems (sUAS) in the U.S., including operating limitations and the requirement for a Remote Pilot Certificate. City departments may conduct sUAS operations either under Part 107 (and apply for specific waivers when needed) or as public aircraft operations under a Certificate of Waiver or Authorization (COA) tailored to the department, mission, and airspace. Depending on the nature of the UAS operation, departments with certified 107 pilots can choose to operate under 107 rules or a COA, once obtained and depending on the operation and the airspace can offer more flexibility in some cases.
Personal Health Information (PHI)	Health and/or medical information that can be used to distinguish or trace an individual’s identity or medical information either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, including, but not limited to: medical records, medical conditions, and/or medical imaging saved in a patient’s file), medical insurance member numbers.
Personally Identifiable Information (PII)	Any data about an individual maintained by an agency including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Privacy-Enhancing Technology	A technology which collects data about people, while minimizing or eliminating the collection of personally identifiable information (PII) and protected health information (PHI) through methods including, but not limited to, encryption, anonymization, differential privacy, and federated learning; an example of this would be using

	LiDAR instead of a camera to count the number of people entering or leaving a building.
Privacy Officer	The City employee designated by a department as the main point of contact and accountability for privacy. Not all departments will have a Privacy Officer.
Public safety operations	Include public safety and emergency management uses across the full incident lifecycle, as well as routine law enforcement, fire suppression, and emergency medical responses.
Remote Pilot in Command (RPIC)	Individual directly responsible for the safe operation of a sUAS under the FAA's Part 107 regulations. This person must hold a valid Remote Pilot Certificate and has the final authority for the flight, ensuring it doesn't create a hazard to people or property, and that all regulations are followed.
Small unmanned aircraft (sUAS)	An unmanned aircraft weighing less than 55 pounds on takeoff, including everything that is on board or otherwise attached to the aircraft.
Small unmanned aircraft systems (sUAS)	Small Unmanned Aircraft Systems (sUAS), commonly known as drones, are unmanned aircraft operating below federally navigable airspace. These systems include not only the aircraft itself but also associated support equipment, such as control stations, data links, telemetry, communication, and navigation equipment.
Surveillance Technology Policy	A department-specific or multidepartment policy document approved by the Board of Supervisor pursuant to Chapter 19B of the San Francisco Administrative Code, that includes authorized uses, data retention, and safeguards for unmanned aircraft systems covered by the ordinance.
Temporary Flight Restriction (TFR) Zone	A temporary airspace restriction put in place to protect persons and property from a hazard, such as those found in emergency situations, national security events, or large crowds at sporting events.
Third Party UAS Service Provider	A non-City entity engaged to plan, conduct, or manage UAS operations on the City's behalf, including their pilots and subcontractors. It does not include mutual-aid agencies acting in their own governmental capacity.
UAS Contractor	An individual or company engaged under a formal agreement to provide ongoing, often integrated, UAS-related services or expertise, including operating City-owned UAS.
UAS Program	Department-designated staff with oversight of the UAS program. This role ensures the programs operates in accordance with Federal, State, and local laws and within department policy and guidelines. Responsibilities include: authorizing UAS training for members; manage reporting requirements (both FAA's and those outlined in this policy); xxx. ccc

UAS Traffic Management (UTM)	A collaborative ecosystem for safely managing unmanned aircraft (UA) operations at low altitudes. This ecosystem is built on a framework of regulatory requirements, technical capabilities, and interoperable services to manage and mitigate operational risks. UTM is separate from, but complementary to, traditional air traffic control, and it provides services such as UA flight planning, airspace authorization, real-time surveillance, and deconfliction to prevent collisions with other airspace users and to support efficient operations, especially beyond visual line of sight (BVLOS).
UAS Vendor	A company selling, leasing, or licensing UAS hardware, software, or cloud services (e.g., aircraft, sensors, Remote ID modules, flight management platforms, video hosting and analytics).
Unmanned Aircraft (UA)	An aircraft flown by a pilot via a ground control system, or autonomously through use of an on-board computer, communication links or other any additional equipment. This includes drones deployed through automated systems such as Drone in a Box (DIAB) technologies, where the aircraft may launch, land, recharge, and transmit data with minimal or no on-site human intervention.
Unmanned Aerial System (UAS) /Drone	An unmanned aircraft and its associated elements (including communication links and the components that control the unmanned aircraft) that are required for the safe and efficient operation of the unmanned aircraft in the national airspace system.
Unmanned Aerial Vehicle (UAV)	A small, unmanned aircraft less than 55 lbs.
Visual line of sight	When a Person operating an unmanned aircraft (UA) has an unobstructed view of the UA. The operator must use their own natural vision (which includes vision corrected by standard eyeglasses or contact lenses) to observe the UA.
Visual observer	A person who is designated by the remote pilot in command to assist the remote pilot in command and the person manipulating the flight controls of the small UAS to see and avoid other air traffic or objects aloft or on the ground.

ANNEX A – Safety Protocols Guidance

A. Preflight Safety

Prior to each flight, the remote pilot in command (RPIC) must confirm authorization and aircraft readiness by applying the following mission-specific safety checks:

- **Pre- and post-flight inspections:** UASs should be inspected briefly before and after each flight, to search for the following:
 - Cracks, dents, or damage to the structure of the drone
 - Loose or out-of-place components
 - Obstructions or damage to motor, wiring or landing gear
 - Battery malfunctions or damage.
- **Verify that the planned mission is authorized** under either Part 107 or the department’s Certificate of Authorization (COA);
- **Confirm the drone is in safe operating conditions.** This includes inspecting all flight control systems (i.e., manual, semi-autonomous, and autonomous), and verifying sufficient power is available for the planned mission [14 CFR § 107.15, § 107.49];
- **Ensure UAVs are configured safely** when flying in populated areas, and that the mission complies with Part 107 Subpart D or an equivalent COA provision for operations over people;
- **Document the maximum flight duration per battery type and ensure backup systems** are available for extended missions;
- **Carefully assess the operating environment**, including risks to persons and property in the immediate vicinity both on the surface and in the air [§ 107.49]. This assessment must include:
 - **Airspace status**, including FAA airspace designations, local restrictions, Notices to Airmen (NOTAMs), and Temporary Flight Restrictions (TFRs);
 - **Local weather conditions** (forecast and observed);
 - **The location of persons and property on the surface;**
 - **Other hazards**, including terrain-induced effects (upslope/downslope winds, leeside rotor/turbulence, wind shear in saddles and canyons) and potential signal occlusion or shadowing from ridges, cliffs, or structures.

B. In-Flight Safety

During flight, each UAS and personnel operating it must meet these minimum operating standards:

- **Crew requirements:** Whenever possible, each UAS flight should include at least two qualified personnel. One individual shall serve as the RPIC with primary control of the aircraft, and the second shall serve as a visual observer (who may also operate the camera, for UAS with separate flight and camera controls).
- **Simultaneous control:** One RPIC may fly multiple UASs only when their routes are fully de-conflicted and a Part 107 waiver or COA expressly authorizes such operations;
- **No distracting features:** UAS must not have features (e.g., lights, coloring) or be flown in a way that distracts motorists, pedestrians, or other air-traffic participants, unless such features are necessary for the success of the UAS operation;

- **GPS loss:** UAS that lose GPS signals shall be automatically set to hover in place until signal is restored or, if safe to do so, an autonomous landing is initiated. Any deviation must be in accordance with an applicable FAA authorization or waiver;
- **Remote ID Function:** The Remote ID function must remain active and shall not be disabled, overridden, or operated in any manner that conceals the aircraft's identity or location (i.e., no "dark operations") unless otherwise permitted, under an FAA authorization, waiver, or exemption;
- **Link loss/low power:** Drones that lose signals to their remote operator or when low power is detected shall be set to return to home/origin;
- **Abort authority:** The RPIC must terminate or abort any flight when mechanical, environmental, or human factors create unsafe conditions;
- **Over-people operations:** When flying over people, a UAS must maintain the minimum altitude and proximity necessary to achieve the mission objective.

C. Operating Limitations

Unless a department's COA grants broader authority, all UAS missions must comply with the following FAA rules:

- **Altitude:** Maximum 400 feet above ground level, or 400 feet above a structure (e.g., bridge structures), if flying within 400 feet laterally [§ 107.51];
- **Groundspeed:** Maximum 87 knots (100 mph) unless a COA authorizes a higher limit and the RPIC documents the justification;
- **Visibility:** At least 3 statute miles;
- **Cloud clearance:** At least 500 feet below and 2,000 feet horizontally;
- **Visual Line of Sights (VLOS):** An aircraft must remain within the unaided VLOS of the RPIC or designated visual observer [14 CFR §107.31 and §107.33];
- **Beyond Visual Line of Sight (BVLOS):** BVLOS UAS operations may be conducted only with an FAA-approved waiver [§ 107.31] or another FAA authorization.
- **Operations near aircraft:** UAS must yield the right-of-way to all aircraft and avoid operating so close to create a collision hazard [§ 107.37];
- **Hazardous operations:** No careless or reckless operations that could endanger life or property; do not drop objects in a manner that creates an undue hazard [§ 107.23];
- **Night operations:** Permitted only if the UAS has anticollision lighting visible ≥ 3 SM (intensity may be reduced if needed for safety);
- **Operations over people:** Prohibited unless the operation satisfies §107.39 or the Subpart D Categories 1–4 requirements (Categories 1: §107.110; 2: §107.115; 3: §107.125; 4: §107.140)
- **Operations over moving vehicles:** Prohibited unless the safety requirements in § 107.145 are met;
- **Highways, freeways, and bridges:** Routine hovering directly above moving vehicles is prohibited to reduce risks from potential mechanical failure or distraction. However, public safety and law enforcement departments may conduct sustained operations above traffic when necessary for emergency response, incident assessment, or traffic management, provided such operations comply with FAA regulations and minimize risk to motorists. Brief, incidental crossing over roadways remains permitted to all departments as part of normal flight paths;
- **Operations in vicinity of airports:** UAS should never be operated in a manner that interferes with operations or traffic patterns at any airport, heliport, or seaplane base. [§ 107.43];

- **Noise:** All UAS operations must use best efforts to avoid generating noise that interferes with the quality of life of City residents or visitors. Operators must comply at all times with the San Francisco Police Code, Article 29 – Regulation of Noise, while flying within City boundaries.

D. Incident Reporting and Corrective Actions

To ensure safety and regulatory compliance, departments must adhere to the following procedures for any UAS-related incident:

- **Grounding:** UASs grounded due to safety concerns shall not be redeployed until the issue is resolved, tested, and documented by authorized maintenance personnel;
- **Incident reporting:** The RPIC must report any safety incident to the department's designated UAS Program Manager within 24 hours of the event, regardless of severity;
- **FAA notification:** When required under 14 CFR § 107.9, the FAA must also be notified;
- **Incident log:** Departments shall maintain an incident log of all safety-related adverse events;
- **Review and corrective actions:** Departments shall conduct an annual audit of incidents to identify root causes and track corrective measures or policy updates taken in response;
- **Audit:** Departments shall conduct periodic audits of the incident log to ensure accuracy, completeness, and timely follow-up on corrective actions. Audits should happen at least once every three months.

E. Preventive Maintenance

To minimize risks to people and property and ensure safe operations, departments must follow the following procedures for all UAS maintenance activities:

- **Scheduled maintenance:** UASs shall follow scheduled preventive maintenance intervals based on manufacturer guidance (e.g., flight hours, cycles, or calendar dates), as well as any FAA or COA-specific requirements;
- **Maintenance log:** A detailed log of all maintenance activities, including date, performed actions, and personnel responsible should be maintained. These records should be retained for a minimum of [xxx] years in accordance with the City's retention policy, and made available for internal audit and risk review.

ANNEX B – No Drone Zone Areas

The City is a complex airspace environment due to a combination of FAA rules and restrictions, local restrictions, and Temporary Flight Restrictions (TFRs). These restrictions are in place to ensure public safety, protect critical infrastructure, and prevent interference with manned aircraft operations. Accordingly, City UAS operations shall observe the following restrictions:

- **Controlled and special-use airspace:** UAS operations in controlled or restricted airspace, including Class B, C, D, or within the lateral boundaries of the surface area of Class E airspace designated for an airport, can be conducted only with all required authorizations (e.g., Air Traffic Control/Low Altitude Authorization and Notification Capability authorization, and any applicable FAA authorization or waiver).
- **Temporary flight restrictions (TFRs):** UAS operations within an active TFR zone (e.g., wildfires, other disaster/hazard areas, major events, fireworks display, VIP movements) may be conducted only with explicit prior approval from the FAA and air traffic control, and have coordinated as required with the controlling agency identified in the restriction notice;
- **SFMTA overhead contact system and yards:** Do not hover over trolley, streetcar, or light rail line wires, above rail, bus and parking control facility yards, unless authorized by the SFMTA.
- **Port of San Francisco (Port):** Do not fly over Port properties subject to the Maritime Transportation Security Act of 2002 (MTSA) without permission from the Port and/or terminal operator;
- **San Francisco Recreation and Park Department:** Do not take launch or land a UAS on SF Recreation & Park property without permission [SF Rec & Park Code §3.09].
- **U.S. Coast Guard facilities, vessels, and security zones:** Do not operate within any active Coast Guard-established security zone without explicit written authorization from the Captain of the Port, including zone established to protect Coast Guard facilities (e.g., Coast Guard Island in Alameda) and naval/Coast Guard vessels [33 CFR § 165.1190]. City UAS operations, including emergency operations, are not automatically exempt and must coordinate with the Coast Guard to obtain a special permit or clearance. Additionally, all operators must comply with FAA special security instructions issued under 14 CFR § 99.7, which require maintaining a stand-off distance of 3,000 feet laterally and 1,000 feet above from U.S. Navy and Coast Guard vessels operating, transiting, or at port within the territorial water and/or navigable waters of the USA.
- **National Park Service (NPS) lands and waters:** Do not launch, land, or operate from or on lands and waters managed by the National Park Service (e.g., the Golden Gate Alcatraz, Fort Point, Crissy Field, Ocean Beach, Baker Beach, Lands End, Fort Funston) without written authorization, such as a Special Use Permit under NPS Policy Memorandum 14-05 [36 CFR § 1.5]. While the NPS may issue expedited approvals during an emergency (e.g., wildfire suppression, search and rescue), City UAS operations are not automatically exempt and must coordinate with the NPS.
- **Presidio Trust Lands:** Do not operate on Presidio Trust–managed lands unless expressly authorized in writing through a Special Use Permit or similar agreement, as required under 36 CFR § 1002.50 and § 1005.3.
- **State Highway System (Caltrans):** Do not operate within the State Highway System without a Caltrans authorization through an encroachment permit or Right-of-Way Use Agreement, under Cal. Code Regs., Title 21, § 1411 et seq.
- **Golden Gate Bridge District:** Do not fly over or near the Bridge or other District property, and signs are posted on site.

- **Jails, juvenile halls, state prisons:** Do not fly over or within jail, juvenile hall, or state prison grounds. This is prohibited under California Penal Code § 4577, except for specific authorized uses.
- **National-security sensitive facilities:** Do not fly from the surface up to 400 ft AGL over designated national security sensitive facilities such as military bases designated as Department of Defense facilities, National landmarks, and certain critical infrastructure, [§ 99.7]. For an accurate list, see FAA map/data of restricted security sensitive airspace.
- **Stadium TFRs during events (e.g., Oracle Park for MLB games):** Do not fly within 3 nautical miles (NM) of the event site, up to 3,000 feet above ground level (AGL), from 1 hour before until 1 hour after the event, including MLB, NFL, NCAA Division I football, NASCAR, and IndyCar.

DRAFT