Table of Contents

OPERATIONS MANUAL

STANDARD INSTRUCTION 02: SPECIALIZED RESPONSE GUIDELINES

SECTION 46: UNMANNED AIRCRAFT SYSTEM

PART 03: DATA COLLECTION

I. PURPOSE

This policy outlines the procedures of collection, use, dissemination and retention of data gathered from the unmanned aircraft system (UAS) program.

II. SCOPE

This policy shall apply to all San Diego Fire-Rescue Department (SDFD) personnel.

III. AUTHORITY

The fire chief authorizes the information within this policy.

IV. DEFINITIONS

A. Digital Multimedia Evidence (DME)**:** Digital multimedia evidence is forensic information of probative value stored or transmitted in digital form.

B. Data Collection: Data collection means to collect and store digital media evidence, or other imagery or data using an unmanned aircraft.

C. Personally Identifiable Information (PII)**:** 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.

D. Privacy Incident: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized users and for unauthorized purpose, have access or potential access to PII in usable form, whether physical or electronic. This term encompasses both suspected and confirmed incidents, whether intentional of inadvertent, involving PII which raise a reasonable risk of harm.

E. Unmanned Aircraft: An aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

F. Unmanned Aircraft System (UAS): An unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.

V. POLICY

A. The City of San Diego is committed to the continued protection of civil liberties, rights, and privacies of individuals.

B. UAS missions must comply with all local, state, and federal laws and regulations, and make reasonable effort to avoid collection, use, or sharing of sensitive data, particularly as it relates to PII, unless authorized by law.

C. UAS may not be used to violate an individual's reasonable expectation of privacy, unless authorized by law.

D. UAS may only be used in a geographically-confined, time-limited emergency situation in which lives are at risk, such as, but not limited to, a fire, hostage crisis, or a search and rescue mission.

VI. PUBLIC NOTIFICATION OF OPERATIONS

A. Notice of all UAS mission operations must be provided to the public when possible. Prior to any mission operation, the UAS program manager must notify the department Public Information Officer of the date, time, and location of operations for distribution through the following channels:

1. City of San Diego Fire-Rescue Department Twitter

2. City of San Diego Fire-Rescue Department Facebook Page

3. Posting on the City of San Diego website

4. Other means of communication deemed reasonable to notify the public

VII. MAINTENANCE AND REFERENCES

A. This document must be reviewed at least annually and updated as appropriate.

B. The UAS program manager must conduct an annual review of UAS operations to verify compliance with stated privacy policy and practices.

C. Annual reviews of this policy shall include, but is not limited to federal, state, and local laws and regulations, as well as the following:

1. Department of Homeland Security Privacy Office, Handbook for Safeguarding PII

2. National Fire Protection Association, NFPA 2400: Standard for Small Unmanned Aircraft Systems (sUAS) used for Public Safety Operations

3. 18 U.S. Code §2510, 2701, 3121, 1367, Electronic Communications Privacy Act of 1986

4. California Constitution Article 1, Declaration of Rights

5. California Civil Code §1708.8, Physical and Constructive Invasions of Privacy

6. California Civil Code §1798.18, Information Practices Act of 1977

7. California Government Code §6250, California Public Records Act

8. California Government Code §34090, Government of Cities

9. San Diego Municipal Code §22.26, Procedures Governing the Management of City Records

10. San Diego Municipal Code 55.54, Unmanned Aircraft Systems

11. City of San Diego Administrative Regulation 85.10, Records Management, Retention and Disposition

12. City of San Diego Administrative Regulation 95.20, Public Records Act Requests and Civil Subpoenas; Procedures for Furnishing Documents and Recovering Costs

VIII. DATA COLLECTION AND RETENTION

A. The agency shall only collect data using UAS, or use UAS-collected data, to the extent that such collection or use is a benefit to the public and is collected consistent with legal authorities.

B. Data obtained may not be used for the following without consent: employment eligibility, promotion, or retention; credit eligibility; or health treatment eligibility unless expressly permitted by and subject to requirements of a regulatory framework. The collection, use, retention, or dissemination of data shall not be used to violate the Constitutional rights of any person, or in any manner that would discriminate against any person based upon their ethnicity, race, gender, national origin, religion, sexual orientation or gender identity.

C. DME Retention and Management

1. The manner in which the DME is stored by the UAS as it is being captured will dictate how the evidence will be secured. If the evidence is stored on a removable device, that device shall be secured at the completion of each mission by the flight crewmember that obtained the evidence. The crewmember will document the date, time, location, and incident numbers or other mission identifiers and the crewmembers involved in mission. This evidence shall be handled in accordance with agency evidence procedures.

2. If the DME is stored on the system hard drive, it shall be handled in accordance with accepted forensic standards for DME without the need to remove the actual storage device.

3. As with all evidence, unauthorized personnel shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute DME.

4. All access to DME must be specifically authorized by agency policy and in accordance with proper evidence handling procedures. The chain of custody documentation for the DME allows for necessary auditing to ensure that only authorized users are accessing the data for legitimate purposes.

5. DME submitted as evidence in a judicial proceeding is, in many cases, no longer in the custody of the agency and shall be handled in accordance with the rules of the court.

D. Digitally Recorded Imagery Not Considered DME

1. All digitally recorded imagery (video, or still photography), or other data, not required as evidence or for use in an on-going investigation shall be managed and disposed of in accordance with federal and state laws, San Diego Municipal Code, and City Administrative Regulation 85.10, *Records Management, Retention and Disposition*.

2. Agency personnel shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute UAS imagery in any manner without their supervisor's approval and in accordance with agency policies.

3. Unless exempt by law, or investigative restrictions, images should be available for public inspection.

E. Personally Identifiable Information (PII)

1. Files containing PII shall be retained in accordance with agency policy, but for no longer than 180 days unless retention of the information is determined to be necessary to an authorized mission of the agency.

2. To retain PII more than 180 days requires documentation stating the reason, estimated length of time the PII will be needed and supervisory approval.

3. PII that becomes DME shall be handled in accordance with the procedures for DME.

IX. PRIVACY INCIDENT REPORTING AND REDRESS

A. All crewmembers associated with a UAS mission in which there has been a privacy incident must report the incident to the San Diego Fire-Rescue Department UAS Program Manager. Upon notification, the UAS Program Manager will work with the City Attorney's Office to provide required notification(s) to the individual(s) affected and meet any mandated reporting requirements.

B. If the privacy incident is related to a system breach, crewmembers associated with the UAS mission must also report the incident to the City's Chief Information Security Officer at cybersecurity@sandiego.gov.

C. Upon discovery of a privacy incident, crewmembers involved in the UAS mission must document or maintain records of information and actions relevant to the incident, as they may be required for investigation of the incident.

D. In the event a member of the public requests redress from the City, the resident(s) will be referred to the City Risk Management Department, Public Liability Division. The resident(s) may complete a "Claim Against the City of San Diego" form to open a claim and/or contact the Risk Management Department at (619) 236-6670. The claim(s) will be reviewed and handled in accordance with processes for all other types of claims against the City.

X. PUBLIC COMMENTS

A. Individuals have the right to find out what information, if any, about the person is in a record and how it is used; correct or amend a record of PII, and report alleged UAS operation misconduct. Comments, complaints, and requests may be submitted through the following:

1. City of San Diego Get It Done phone application under "Other"
2. City of San Diego "Get It Done" webpage
3. Email to UnmannedSystems@sandiego.gov