



POLICY DIRECTIVE

Policy:	DOC 3.1.39 SMALL UNMANNED AIRCRAFT SYSTEMS (sUAS) OPERATIONS	
Effective Date:	09/04/2026	Page 1 of 7
Revision Date(s):		
Signature(s):	/s/ John Schaffer, Public Safety Chief	

I. POLICY

This policy establishes guidelines for the use of Small Unmanned Aircraft Systems (sUAS) by the Department to improve overall security, enhance the safety of staff and the public, and increase situational awareness during critical events.

II. PURPOSE AND APPLICABILITY

The purpose of this policy is to provide direction for the authorized use of sUAS in accordance with applicable laws, regulations, and Department standards. This policy applies to all Department employees who operate, supervise, authorize, or support unmanned aircraft activities for official business.

III. DEFINITIONS (see Glossary)

IV. OBJECTIVES

A. Responsible sUAS Use

The Department will ensure that sUAS are used responsibly, transparently, and securely. To uphold these principles, the Department establishes the following framework:

1. **Transparent Oversight and Accountability:**

The Department will operate the sUAS program with robust internal and external oversight in order to ensure compliance with all applicable laws, policies, and procedures.

2. **Community Engagement and Transparency:**

Where appropriate and when it does not compromise facility security, operational integrity, or ongoing investigations, the Department will engage with the public regarding sUAS use for Department-approved functions to promote transparency.

3. **Civil Liberties and Privacy Protection:**

The Department will implement operational safeguards, training, and audit mechanisms to prevent misuse and ensure that any data collected is handled in an ethical manner, consistent with federal aviation privacy guidance for sUAS operators in accordance with 14 C.F.R. § 107.100 et seq. These safeguards must also comply with Montana privacy and communications statutes and state agency personal information protection requirements that are outlined in §§ 2-6-1502 and 45-8-213, MCA, and consistent with *DOC 1.5.20 Record Retention*, and *DOC 1.7.3 Data Quality* policies.

4. **Standardized Operating Procedures:**

Department policy and training will establish standardized operating policies that rely on and adherence to the law, FAA compliance, and data integrity. The policies and training will cover all pre-flight checks, flight planning, data administration, and post-flight reviews.

5. **Cybersecurity:**

The sUAS program will conduct regular security reviews and protect all related systems against unauthorized access while safeguarding sensitive data.

- a. All sUAS platforms and supporting systems must comply with Montana State Information Technology Services Division (SITSD) security policies and standards, including internet privacy and security requirements, encryption in transit and at rest, and incident reporting procedures.
- b. Cybersecurity safeguards for sUAS data shall align with the Department's data governance and records policies, enumerated in *DOC 1.5.20 Records Retention*, and *DOC 1.7.3 Data Quality*.

V. OVERSIGHT AND ACCOUNTABILITY

A. Department sUAS Oversight Committee

A cross-functional committee led by the Security Technology Specialist and consisting of representatives from:

1. Facilities, such as the Wardens or their designees;
2. The Department's IT/SITSD liaison;
3. Training Bureau;
4. Emergency Preparedness Division;
5. Legal Services; and
6. Investigations Bureau.

B. Committee Responsibilities

The committee shall:

1. Review and approve or deny proposals for sUAS use, qualifications, and training requirements;
2. Review and update as necessary sUAS training, qualifications, and policies annually;
3. Provide oversight for the procurement, insurance, maintenance, and lifecycle replacements of sUAS assets in coordination with procurement and budgeting processes;
4. Evaluate program data, deployment summaries, incident reports, and performance metrics;
5. Ensure compliance with privacy protections, cybersecurity standards, and state and federal regulations;
6. Prepare reports for executive leadership; and
7. Support community engagement when appropriate, public information requests, and transparency reporting.

C. sUAS Program Manager

The Department sUAS Program Manager is responsible for overall administrative and operational control of the Department's sUAS program. The sUAS Program Manager will:

1. Apply for, manage, and maintain FAA authorizations, including Part 107 waivers and Certificates of Authorization (COAs);
2. Develop program budgets, plan for equipment lifecycle replacements, and identify funding sources;
3. Coordinate procurement of sUAS, docks, batteries, accessories, support equipment, and related technology;
4. Develop and implement statewide strategies for sUAS use across Department operations;

5. Ensure all Remote Pilots and Visual Observers are appropriately trained and certified;
6. Oversee data policies and security in coordination with Department IT;
7. Support integration with other Department technologies, including surveillance, incident command, and emergency management platforms;
8. Investigate and document any sUAS-related incidents, safety violations, policy breaches, or cybersecurity events, and report findings to the Committee and executive leadership; and
9. Serve as the Department's primary liaison with the FAA, SITSD, and external sUAS regulatory and oversight entities.

D. Remote Pilots and Visual Observers

1. All Department-authorized Remote Pilots and visual observers must:
 - a. Hold a valid FAA Part 107 certification unless operating exclusively under an approved COA with internal certification requirements;
 - b. Complete all Department-required sUAS training, including initial training, annual refresher training, and proficiency evaluations;
 - c. Demonstrate knowledge of and comply with all Department, FAA, and facility-specific requirements and restrictions governing sUAS operations; and
 - d. Consistently demonstrate actions that comport with safe, compliant, and properly documented flight operations.
2. Authorization and designation:
 - a. The sUAS Program Manager will maintain a current roster of Department-authorized Remote Pilots and visual observers, including certification number and status, training dates, and any restrictions on operations.
 - b. Requests for authorization of employees to operate sUAS must be submitted to the sUAS Program Manager who will verify qualifications, coordinate required training, and issue written authorization upon successful completion of all requirements.
 - c. Authorization may be suspended or revoked by the sUAS Program Manager or facility administrators in coordination with the sUAS Program Manager due to any of the following reasons:
 - 1) Safety violations or unsafe operating practices;
 - 2) Non-compliance with Department policies;
 - 3) Loss, expiration, or suspension of required certifications or Department training qualifications or failure to maintain required proficiency standards;
 - 4) Pending investigations into sUAS-related incidents, privacy violations, data breaches, or other misconduct; or
 - 5) Any other cause determined by the sUAS Program Manager to compromise safety, security, legal compliance, or program integrity.
 - d. Only individuals listed as current authorized Remote Pilots or visual observers on the current roster may operate or support sUAS missions.

VI. COMMUNITY ENGAGEMENT AND TRANSPARENCY

A. Community Engagement

1. Outreach opportunities may include:
 - a. Demonstrations and informational sessions during job fairs, public safety events, or community open houses;
 - b. STEM-based educational partnerships; and
 - c. Leadership briefings for state officials and oversight bodies.

2. Community engagement activities will not disclose sensitive security information, including specific security infrastructure locations, detailed operational tactics, vulnerabilities, or information that could reasonably be used to compromise facility security or public safety.

B. Transparency

1. The Department may establish a public-facing sUAS information portal summarizing:
 - a. Authorized use cases and mission categories;
 - b. Training and proficiency standards;
 - c. Annual sUAS operational statistics, including total flight hours, number of deployments by use-case category, and general geographic areas of operation; and
 - d. Privacy safeguards and data retention practices in summary form.

C. Privacy

1. Department sUAS operations shall protect the privacy and civil liberties of staff, offenders, contractors, visitors, and the public. Except as authorized by exigent circumstances, court order, or other lawful authority:
 - a. Operators will not intentionally record or surveil individual in areas or circumstances where those individuals have a reasonable expectation of privacy;
 - b. Operators will take reasonable precautions to minimize unnecessary or incidental collections of images, video, audio, or other personal data unrelated to the authorized mission purpose; and
 - c. Collected imagery will be used only for authorized Department purposes, such as investigations, incident documentation, security monitoring, training, or emergency response, infrastructure inspection, and other lawful operational needs.
2. Sensitive areas, including but not limited to staff bathrooms, medical examination or treatment rooms, mental health counseling areas, attorney-client meeting or call locations, may not be intentionally recorded or monitored via sUAS except:
 - a. When necessary to address an imminent threat to life, serious bodily injury, or critical facility security under exigent circumstances;
 - b. Pursuant to a valid court order or warrant; or
 - c. With the informed, voluntary, and documented consent of all individuals whose privacy would be affected.
3. When incidental collection of images or data depicting individuals in sensitive areas or private circumstances occurs during sUAS use, the Remote Pilot or Program Manager will:
 - a. Cease recording or reposition the sUAS to avoid continued incidental collection, unless doing so would compromise safety or the mission objective;
 - b. Document the incident collection in the post-flight report; and
 - c. Ensure that incidental data is redacted or anonymized unless retention required for a legitimate investigative, evidentiary, or security purpose.

D. Annual Privacy and Compliance Assessment

1. The sUAS Oversight Committee shall undertake a comprehensive annual assessment that encompasses a thorough examination of:
 - a. Relevant state and federal privacy laws;
 - b. Department policies;
 - c. FAA regulatory changes; and
 - d. Internal operational practices including review of deployment logs, incident reports, privacy complaints, and data-handling audits; and
 - e. Emerging best practices and regulatory guidance affecting government sUAS operations and privacy protections.
2. The sUAS Oversight Committee will prepare a written assessment report documenting findings, identified compliance gaps, and recommend policy or operational changes.

3. All recommendations issued by the sUAS Oversight Committee shall be formally submitted to the Department's executive leadership for review, approval, and implementation direction.

E. Procurement

1. All sUAS procurement must comply with:
 - a. State of Montana procurement rules, and;
 - b. Department purchasing procedures and approved standard equipment lists; and
 - c. Federal cybersecurity requirements, including restriction to Blue UAS/sUAS cleared list platforms or systems approved for and meeting federal supply-chain security standards.
2. The sUAS Program Manager shall maintain a current inventory of all Department sUAS platforms, batteries, accessories, docking stations, ground control systems, and support equipment, including serial numbers, acquisition dates, warranty information, and operational status and develop and maintain a lifecycle replacement plan identifying anticipated equipment replacement timelines and associated budget requirements.

VII. OPERATING PROCEDURES

A. General Guidelines

While operating a sUAS/UAS the operator(s) will comply with the following guidelines:

1. Strict observance of the Department's sUAS General Operating Manual (GOM) is required for all sUAS/UAS operations.
2. Operators must comply with facility-specific Standard Operating Procedures (SOPs) tailored to their location and mission.
3. All activities shall conform to FAA Part 107 requirements governing unmanned aircraft systems.
4. Relevant COA provisions must be fully observed during operations.
5. The Department Code of Conduct serves as a foundational guideline for operator behavior and professionalism.
6. State of Montana IT security standards must be rigorously followed to ensure data protection and system integrity.
7. Operators are required to implement and uphold SITSD cybersecurity protocols throughout all sUAS-related activities.
8. No operator may deviate from these standards unless it is necessary to prevent immediate harm. Any emergency deviation must be documented immediately in the post-flight report and reported to the sUAS Program Manager and facility administrator within 24 hours.

B. Authorized Uses

Department-authorized operators may deploy sUAS for the following categories of qualifying events and operational purposes:

1. **Critical Incidents.** sUAS may be deployed in response to critical incidents posing an immediate or imminent threat to life, safety, or facility security, including:
 - a. Escapes, or attempted escapes from secure facilities or custody;
 - b. Hostage situations or barricaded-subject incidents;
 - c. Riot, disturbance, or large-scale disorder monitoring and tactical assessment;
 - d. Contraband delivery attempts, including detection and interdiction of unauthorized drone deliveries;
 - e. Staff assault, use -of-force incidents, or officer-safety emergencies requiring aerial observation or documentation; and

- f. Suspected unauthorized drone incursions over secure airspace or restricted facility perimeters.
- 2. **Perimeter and Security Operations.** sUAS may be deployed for routine and enhanced security operations, including:
 - a. Fenceline inspections and perimeter integrity assessments;
 - b. Perimeter breach detection and response;
 - c. Counter -UAS monitoring tracking, and threat assessment;
 - d. Night operations or thermal surveillance to identify security gaps, unauthorized persons, or concealed contraband;
 - e. Search and rescue operations and life-safety missions;
 - f. Missing person searches, including searches for individuals who have eloped from prerelease centers, work-release programs, or community custody; and
 - g. Natural disaster response, damage assessment, and emergency evacuation support.
- 3. **Investigations and Evidence Collection.** sUAS maybe deployed to support criminal, administrative, or incident investigations, including:
 - a. Crime scene recording and documentation;
 - b. Use-of-force documentation and reconstruction;
 - c. Facility damage assessments following incidents, natural events, or suspected sabotage; and
 - d. Collection of evidence in support of ongoing investigations, subject to applicable search and seizure protections and legal standards.
- 4. **Infrastructure Inspection.** sUAS may be deployed to for infrastructure assessment and facility management purposes, including:
 - a. Roof inspections for damage, leaks, or structural integrity;
 - b. Tower, antenna, and utility infrastructure mapping, inspection, and maintenance planning; and
 - c. Environmental assessments, including but not limited to vegetation management, erosion monitoring, and stormwater infrastructure evaluation; and
 - d. Wildfire risk assessments and fuel-load mapping.
- 5. **Training and Readiness.** sUAS may be deployed for training, certification, proficiency maintenance, and equipment testing purposes, including:
 - a. Initial and recurrent Remote Pilot certification and proficiency flights;
 - b. Monthly or quarterly proficiency evaluations and skills maintenance; and
 - c. Equipment testing, system integration validation, and technology evaluations, including Skydio Hive deployments; and
 - d. Training exercises, tabletop simulations, and emergency preparedness drills.

C. Prohibited Uses

- 1. The Department will not use sUAS for the following purposes:
 - a. Random, indiscriminate, or generalized of staff, visitors, or the general public, except as necessary for routine facility perimeter security patrols, infrastructure inspections, or active incident response;
 - 1) Unintentional or incidental recordings and/or observations are excepted.
 - b. Monitoring employee activities for disciplinary purposes or performance-evaluation purposes in the absence of reasonable suspicion of misconduct, policy violation, or criminal activity;
 - c. Any surveillance, recording, or data collection unrelated to legitimate Department authorized use;
 - d. Activities that violate federal or state law; and
 - e. Any form of weaponization of the sUAS platforms, including the mounting, deployment or use of chemical agents, kinetic projectiles, or electrical discharge devices, or any other

weapons or munitions, unless explicitly authorized by federal statute and approved by the Department's executive leadership and legal counsel.

VIII. sUAS DATA, CYBERSECURITY AND RETENTION

A. Guidelines

1. All sUAS data shall be handled in compliance with:
 - a. Department data governance policy as enumerated in *DOC 1.7.3 Data Quality*;
 - b. State of Montana SITSD Security policy;
 - c. Criminal Justice Information Services (CJIS) Security Policy requirements where applicable; and
 - d. All additional Department-approved digital evidence management systems and chain-of-custody protocols.
2. Data management requirements:
 - a. All flight imagery, video, and sensor data must be uploaded and tagged with an approved evidence or storage system.
 - b. Retention schedules shall align with *DOC 1.5.20 Records Retention* policy.
 - c. Unauthorized storage on personal devices is strictly prohibited.
 - d. All data must remain encrypted in transit and at rest.
 - e. Access shall be restricted to individuals with appropriate security clearance, role-based authorization, and a legitimate business need.

IX. CLOSING

All questions about the sUAS drone operations should be directed to Public Safety Chief.

X. REFERENCES

- A. *14 C.F.R. § 107*
- B. *§§ 2-6-1502 and 45-8-213, MCA*
- C. *DOC 1.5.20 Records Retention; DOC 1.7.3 Data Quality*